

IBM Guardium Data Protection 12.x



Tables of Contents

Welcome	1
Product overview	1
IBM Guardium	1
What's new in this release	2
Release information	5
Product legal notices	6
Trademarks	7
Terms and conditions for product documentation	7
Privacy policy considerations	7
FIPS 140-2	7
Getting started	8
Components and topology	8
Getting started with the user interface	9
Customizing the User Interface	10
Identifying and investigating risks: getting started	10
Smart assistant for monitoring and compliance	10
System view	11
Data activity monitoring	11
Policies and rules	12
Workflows	12
Auditing	12
Classification	12
File activity monitoring on Windows and Unix-Linux file servers	12
File activity monitoring functionality	12
High level workflow for file activity monitoring	14
File activity monitoring for NAS and SharePoint	14
Key concepts and tools	15
Queries and reports	15
Access control	15
User roles	15
Groups	15
Data archive and purge	16
Guardium Installation Manager	16
Discover	16
Datasources	17
Creating a datasource definition	17
Creating a datasource group	18
Configuring your datasource	19
Amazon DynamoDB	20
Amazon Redshift	20
Apache Cassandra	21
Aster	22
Cloudera Manager	22
CockroachDB	23
Couchbase	23
DataStax Cassandra	24
Db2	25
Db2 for i	25
Db2 for z/OS	26
EDB PostgreSQL	26
GreenplumDB	27
Guardium Big Data Intelligence	27
Hive	28
Informix	28
MariaDB	29
MongoDB	30
MS SQL Server (DataDirect - Dynamic Port)	31
MS SQL Server (DataDirect)	32
MS SQL Server (Microsoft - Dynamic Port)	34
MS SQL Server (Microsoft)	35
MySQL	36
Neo4j	38
Netezza	39
Oracle (Data Direct - Service Name)	39
Oracle (Data Direct - SID)	41
Percona MySQL	42
PostgreSQL	43
SAP HANA	43
Snowflake	44
SQL DB Azure	45

Sybase	45
Sybase IQ	46
TERADATA	46
Text datasources	47
Configuring custom properties for your datasources	47
Working with existing datasources	48
Reporting on datasources	48
Defining a datasource using a service name	48
Managing KDC definitions	49
Managing datasource credentials with CyberArk	49
CyberArk deployment overview	50
Setting up the CyberArk vault system	50
Creating an application ID on CyberArk	50
Adding and removing account permissions on CyberArk	51
Deploying CyberArk on your Guardium system	51
Downloading and installing the CyberArk SDK patch	52
Installing CyberArk	52
Configuring CyberArk on your Guardium system	52
Defining Guardium datasources to access CyberArk	53
Upgrading the CyberArk SDK on a central manager or standalone system	53
Upgrading the CyberArk SDK on a managed unit	53
Uninstalling CyberArk	54
Managing datasource credentials with AWS Secrets Manager	54
Gathering required information	54
Creating a secret user	55
Creating a secret key	55
Selecting the authentication type and setting up roles	55
Authenticating by using security credentials	56
Authenticating by using IAM Role	56
Authenticating by using IAM Role for AWS Secrets Manager	56
Authenticating by using IAM Role for AWS database service	57
Authenticating by using IAM instance profile	58
Configuring the AWS Secrets Manager on your Guardium system	58
Defining Guardium datasources to access AWS Secret Manager	59
Managing datasource credentials with HashiCorp	60
Gathering required information	60
Creating a HashiCorp Policy	60
Creating and importing a client certificate	61
Configuring HashiCorp on your Guardium system	63
Defining Guardium datasources to access the HashiCorp vault	64
Database Auto-discovery	64
Cloud database service protection	65
Cloud database service protection Amazon AWS setup	66
Define AWS IAM for data streams	66
Define, modify, and delete AWS cloud DB service accounts	67
Discover and configure AWS data streams	68
Manage AWS data streams	68
Cloud database service protection Azure setup	69
Define, modify, and delete Azure cloud database service accounts	70
Monitor Azure event hubs	71
Manage Azure event hubs	72
Cloud database service protection with native audit	72
Cloud database service protection workflow	73
Define AWS IAM for native audit	74
Create, modify, delete cloud accounts	74
Discover cloud databases	75
Catalog and manage databases	76
Manage Classification and Vulnerability Assessment	76
Configure database auditing	77
Manage object auditing	79
Managing object audit in one database	79
Managing object audit in multiple databases	79
Database discovered instances rules	80
Database discovered instance rules scheduler	82
Adding reports and alerts for inspection engine changes	82
Classification	83
Classification process performance	83
Classification Rule Handling	84
Discover Sensitive Data	84
Discovery scenarios	85
Name and description	86
What to discover	86
Rule Criteria	87
Actual Member Content	88

Where to search	89
Run discovery and review report	89
Remove false-positives from discovery results	90
Audit	91
Scheduling	91
Runtime sensitive-object identification	92
Regular Expressions	92
FAM discovery and classification in Windows and UNIX-Linux file servers	93
Installing and activating the FAM discovery agent (crawler) on UNIX servers	93
Installing and activating FAM discovery agent (crawler) on Windows servers	94
File discovery and classification GIM parameters	95
Rules for GDPR File Activity	96
File discovery and classification for NAS and SharePoint	97
Supported platforms	98
Scan Permissions	98
Installing client software	100
Configure Scan Settings	100
View Scan Results	101
Creating User-Defined Criteria	102
Entitlement Optimization	102
Enable and configure entitlement optimization	103
Entitlement Optimization What's New	103
Entitlement Optimization Users and Roles	104
Entitlement Optimization Recommendations	104
Entitlement Optimization Browse entitlements	104
Entitlement Optimization What If	105
Protect	106
Active Threat Analytics	106
Threat descriptions	107
Creating threat categories from policy rules	109
Excluding items from Active Threat Analytics	109
Active Threat Analytics setup	110
Risk Spotter	111
Risk Spotter functions	112
Risk Spotter risk indicators	112
Use the Risk Spotter results	113
Create a Dynamic Auditing policy	114
Configure and enable Risk Spotter	115
Outliers detection	116
Quick start for outlier detection	117
Enabling and disabling outliers detection	117
Interpreting data outliers in the investigation dashboard	118
Interpreting file activity outliers in the investigation dashboard	119
Switching DB and OS users	120
Grouping users and objects for outliers detection	121
Outliers detection clustering	121
Real-time trust evaluator	121
Configuring the trust evaluator	122
Viewing trust evaluator status	124
Adding post-training automation	124
Configuring the connections table	124
Policies	125
Understanding policies	125
Rule types, categories, classifications	126
Minimum counts and reset intervals	126
Continue to next rule	126
Record values with policy violation	126
Values and groups of values in rules	127
Matching patterns with regular expressions	127
Special pattern tests	127
Log flat	128
Rules on flat	128
Selective audit trail	128
Analyzer rules	129
Character sets	129
Session-level policies	146
Creating session-level and advanced session-level policies	147
Creating session-level policies	147
Creating tuple parameters for session-level policies	148
Creating advanced session-level policies	148
Using session-level and advanced session-level policies	149
Wildcards	149
Tokens	150
IPv6 support	151
Groups	151
Grammar	152

Unsupported databases for session-level policies	153
Criteria	153
Tuples	156
Actions	157
Audit and ignore session actions	157
Mark session actions	158
Alert and Log actions	159
Parse actions	159
Configure actions	159
Transform actions	160
Transform parameters	162
Exception actions	162
Extrusion actions	163
Action parameters	163
Label action and criteria	163
Distinct parameter	164
Track option	165
Search parameters	165
Session-level policy examples	166
Ignoring sessions example	169
Log LOGIN_FAILED sessions only example	170
REQUEST_ERROR example	170
Add DB name on failed login example	170
Get correct service name (MS SQL Server) example	170
Ignoring exceptions examples	171
Firewall and latency issues examples	172
Sniffer overload issues examples	173
Query masking examples	174
Correct IP address (Oracle) example	175
Show SQL schema names example	175
Server and S-TAP IP addresses example	176
User authentication (Oracle) example	177
Redacting data example	177
Hostname caching example	178
Ignore specified users example (MongoDB)	178
Scheduling with SESSION_START examples	179
Logging access activity for trusted sessions example	180
Creating a custom exception message example	180
Find name in SQL query example	181
Detect local admin example	181
Strict username example (Oracle)	182
Login information dump example	182
Known limitations	183
Policy rule actions	183
Blocking rule actions	183
Alerting rule actions	184
Logging or ignoring rule actions	185
Understanding ignore actions	186
Log full details	188
Set character set	188
Rule definition fields	189
Creating and installing a policy and policy rules	192
Tagging policy rules	193
Importing rules by tag	193
Adding tags while defining policy rules	194
Managing policy rule tags	194
Using the Policy Installation tool	194
Running policy analyzer and reviewing results	195
Security incident policies	196
Security anomalies	196
Access to unaudited sensitive data	197
Administrative user accessing sensitive data	197
Administrative users and applications	197
All users	198
Credential stuffing attack	199
Repeated failed logins or possible denial of service attack	199
Suspicious user activity with sensitive data (user not privileged)	200
Quarantine users with multiple failed logins	200
Managing correlation alerts	200
Incident Management	202
How to manage the review of multiple database security incidents	203
Query rewrite	205
How query rewrite works	206

Using query rewrite	207
Enabling query rewrite	207
Creating query rewrite definitions	207
Testing query rewrite definitions	208
Defining a security policy to activate query rewrite	209
Creating a custom report to validate query rewrite results	210
File Activity policies for UNIX and Windows file servers	210
Using rules for file activity policies	210
Create a FAM policy and its rules from scratch for Windows and UNIX servers	212
Creating a FAM policy rule from the Investigative Dashboard Entitlements tab	213
File activity policies for network-attached storage (NAS) and SharePoint	213
Creating file activity policies for network-attached storage (NAS) devices	213
Creating file activity policies for SharePoint	214
Creating a DAM access policy to monitor files on NAS and SharePoint	214
Configuring consolidation of FAM MS Office events	215
Investigation Dashboard for data	216
Filtering data and saving filters in the investigation dashboard	217
Monitor and audit	218
Enabling and disabling the Investigation Dashboard	219
Basic data security monitoring policy	219
Prerequisites	220
Install the basic data security monitoring policy	220
Understand the basic data security monitoring policy rules	221
Create reports for basic data security monitoring	221
Create an Admin Users Activity report	222
Create an Administration Commands Execution report	222
Next steps for data security monitoring	222
Smart assistant for compliance monitoring	223
Databases	223
Add an individual database	224
Import multiple databases	224
Reconciling database inventory	225
Applications	226
Add an individual application	226
Import multiple applications	227
Compliance summary	227
Application summary	228
Set up compliance monitoring or application data monitoring	228
Prerequisites	228
Select compliance type	229
Select databases or applications to monitor	229
Search for sensitive data	229
Summary	230
Investigation Dashboards	230
Enabling File Activity in the investigation dashboard	231
Accessing the investigation dashboard	231
Using the Sankey chart	232
Using Data In-Sight	232
Investigation Dashboard for files	233
Filtering data and saving filters in the investigation dashboard	217
Filtering an individual chart	235
Creating, saving, and exporting investigation dashboards	235
Using the topology view	236
Local and distributed search	237
Monitoring and automatic recovery for the Investigation Dashboard	237
Viewing the Investigation Dashboard's status in deployment health views	237
Viewing Investigation Dashboard issues in reports	237
Viewing the Investigation Dashboard Issues alert for the Investigation dashboard	238
Addressing Investigation Dashboard issues	238
Running manual intervention for Investigation Dashboard issues	238
Threat Detection Analytics	239
Characteristics of an SQL injection attack	240
Characteristics of a stored procedure attack	240
Enabling and disabling threat detection analytics	240
Viewing case reports	241
Activating the audit process workflow for threat analytics	241
Working with threat diagnostic dashboards	241
Investigating SQL injection threats	242
Investigating stored procedure threats	242
Data Protection Dashboard	243
Building audit processes	244
Audit process task types	246
Audit process receivers	247
Exporting audit results	250
How to distribute workflow through Guardium groups	251

Audit Process To-Do List	259
Comparing discovery and classification results	260
Using the host references report	261
Audit and Report	261
External data correlation	261
Privacy sets	267
Custom Alerting	268
Flat Log Process	270
Running database entitlement reports	270
User Identification	271
Identify Users using the Application User Translation	272
Identify Users with API	276
Identify Users via Stored Procedures	278
Value Change Auditing	279
Creating an Audit Database	280
Monitored Table Access	282
Installing and activating the FamMonitor on Windows servers	283
Install the FamMonitor installation package with the wizard	284
Install the FamMonitor bundle with GIM	284
FamMonitor GIM installation parameters	285
Install and uninstall the FamMonitor installation package with command line	286
FamMonitor command line installation parameters	286
File Activity Monitor for NAS and SharePoint	287
Supported platforms	287
Monitoring Permissions	287
Installation	289
Configuration	289
Viewing Results	289
Uninstallation	290
How to use PCI/DSS Accelerator to implement PCI compliance	290
Workflow Builder	293
How to create Customized Workflows	294
How to use Customized Workflows	295
Opening Workflow Process Results	297
Reports	297
Predefined reports	297
Predefined admin reports	298
Predefined user reports	324
Predefined common reports	331
Creating dashboards and adding reports	333
Opening the investigation dashboard, filtered for report entities	333
Viewing reports	334
Modifying the runtime parameters	335
Refreshing reports	335
Exporting a report	335
Viewing Drill-Down Reports	336
Ad-hoc process for run once now	336
Using the Query-Report Builder	336
Optimizing queries	337
Creating a new query, modifying an existing query	338
Defining the query name and attributes	339
Managing query security roles	339
Adding a query to a datamart	340
Modifying the query drilldown control	340
Modifying the API assignment	340
Selecting the column display	340
Setting the sort order	341
Defining the Query Conditions	341
Adding a build expression on query condition	343
Having conditions	343
Modifying the report display	343
Domains, Entities, and Attributes	344
Entities and Attributes in the domains	344
Access domain	346
Access Policy domain	353
Aggregation/Archive domain	355
Alert domain	356
Analytic Threat Analytics domain	357
Analytic Outlier Details domain	358
Analytic Outliers Status domain	358
Analytic Outlier Summary domain	359
Application Data domain	359
Audit Process domain	362
Auto-discovery domain	363
BigData Intelligence Buff Usage Monitor domain	364
BigData Intelligence Classification Process Log domain	365
BigData Intelligence Classifier Results domain	365

BigData Intelligence Databases Discovered domain	366
BigData Intelligence Discovered Instances domain	366
BigData Intelligence Exception domain	367
BigData Intelligence Full SQL domain	367
BigData Intelligence Installed Patches domain	368
BigData Intelligence Instance domain	368
BigData Intelligence Outliers List Enhanced domain	369
BigData Intelligence Outliers Summary Enhanced domain	370
BigData Intelligence Policy Violations domain	370
BigData Intelligence Session domain	371
BigData Intelligence STAP Status domain	372
BigData Intelligence System Info domain	372
BigData Intelligence VA Results domain	373
CAS Changes domain	373
CAS Config domain	374
CAS Host History domain	375
CAS Templates domain	376
Catalog domain: entities and attributes	376
Classification Process Results domain	377
CM Buffer Usage Monitor domain	378
Comments domain	379
Custom DB Usage domain	379
DB Default Users Enabled domain	380
Discovered Instances domain	380
Distributed Datamart domain	380
Eagle Eye domain	381
Exceptions domain	382
FAM domain	386
FAM groups domain	387
FAM System domain	388
File Activity Monitor domain	388
Flat Log domain	389
GIM Clients domain	392
GIM Events domain	393
Group domain	393
Guard Process Log domain	393
Guardium Activity domain	394
Guardium Jobs Queue domain	394
Guardium Login domain	395
IMS Event domain	395
Installed Patches domain	401
Installed Policy domain	402
Managed units domain	404
Parser Errors domain	404
Policy Violations domain	406
Policy Violations Summary domain	412
Query Rewrite domain	415
Runtime Sensitive Object Identifier domain	418
Security Assessment Result domain	419
Sniffer Buffer Usage Monitor domain	421
S-TAP Status domain	423
S-TAP status history domain	424
S-TAP Statistics domain	424
S-TAP verification domain	425
Unit Utilization Levels domain	425
User/Role/Application domain	426
VA Summary domain	427
VA Tests domain	427
Value Change domain	428
Database Entitlement Reports	429
Custom Domains	438
Data Mart	444
Viewing your data marts	444
Extracting data mart to table	444
Extracting data mart to file	445
Manage predefined data extraction to file	446
Distributed Report Builder	448
Creating a Distributed Report	451
Working with API calls and reports	453
Mapping APIs to report results	454
How to Generate API Call from Reports	454
How to use Constants within API Calls	458
How to use API Calls from Custom Reports	462

Working with external feeds	465
Mapping an External Feed	465
Creating an external feed	466
Creating reports for z/OS	466
Working with Data Sets reports	
Built-in reports for Data Sets	467
Report entities and attributes for Data Sets	467
Working with Db2 for z/OS reports	
Built-in reports for DB2 for z/OS	470
Example reports for DB2 for z/OS	470
Report entities and attributes for DB2 for z/OS	471
Working with IMS reports	
Built-in reports for IMS	473
Example reports for IMS	474
Report entities and attributes for IMS	475
Assess and harden	477
Introducing Guardium Vulnerability Assessment	477
Database privileges for vulnerability assessments and classification	479
Deploying VA for Db2 for i	480
Using VA with Cloudera	481
Troubleshooting Cassandra	484
Set up your environment for Vulnerability Assessment	485
Types of Vulnerability Assessments	485
Defining a query-based test	486
Defining a CAS-based test	487
Assessments	488
Creating an assessment	488
Finding an assessment	489
Running an assessment	489
Viewing assessment results	489
Tuning a test	491
Determining test severity	491
Deleting an assessment	492
Creating a test exception	492
Group exceptions	492
Test detail exceptions	493
Adding custom comments to a test	493
Modifying the database version and patch level	493
VA summary	494
IBM Guardium Data Protection app in ServiceNow	494
Required schema change	495
Assessing RACF vulnerabilities	495
Configuration Auditing System (CAS)	496
CAS server authentication with SSL	498
Prerequisites, installing, and running CAS on a Windows server	498
Installing CAS from the CLI	499
Installing CAS with GIM	499
Prerequisites, installing and running CAS on a Linux, UNIX server	500
Locating the Java home directory and version	501
CAS start-up and failover	502
CAS templates	504
Working with CAS templates	508
CAS hosts	510
CAS reporting	511
CAS status	512
License information for Guardium Vulnerability Assessment	513
Example scenarios	514
Configuring your Guardium system	517
System Configuration	517
Managing data: archive, restore, aggregation, and system backup	519
Planning archiving, storage capacity, and scheduling	520
Managing stored data	523
Configure data archive	523
Archiving (audit) results	524
Restoring archived data	524
Restoring archived data on an empty appliance	525
Restoring a few days of recent data	526
Restoring and viewing audit results in the investigation center	526
Exporting (files) results	527
Viewing days whose data was not archived or exported	528
Data and Result catalogs	528
Import catalog entries	529
Export catalog entries	529
Adding, removing, and modifying catalog entries	529
Data aggregation	530
Exporting data	531

Importing data	532
Purging data	532
Configuring data purge	532
Purging data to resolve a full disk when the GUI is down	533
Configuring system backup	535
Restoring a Guardium system	535
Before you restore your Guardium system	536
Restoring a standalone collector	537
Restoring a collector with an aggregator that is not centrally managed	538
Restoring an aggregator that is not centrally managed	538
Restoring a centrally managed collector	538
Restoring a centrally managed aggregator	539
Restoring a dedicated central manager (no data aggregation)	539
Restoring default and custom certificates	540
Enabling SSH key pairs for data archive, data export, data mart	540
Transferring data to a remote host by using SSH key pairs for authentication	541
Configuring external storage	542
Configure an Amazon S3 (Amazon Simple Storage Service) target for archive or backup	542
Configuring an IBM COS (formerly Cleversafe) target for archive or backup	544
Configure an EMC Centera target for archive or backup	545
Configuring an SCP or SFTP target for archive or backup	545
Configure a Tivoli Storage Manager (TSM) archive or backup	546
Internet Protocol modes	546
Enable IPv4	547
Enable dual IP mode in an existing IPv4 deployment	548
Migrate to IPv6 in an existing IPv4 deployment	548
Enable IPv6 in a new deployment	549
Assign IPv6 addresses to your devices	550
IPv6 limitations, best practices, FAQ, and troubleshooting	550
Network mirroring methods (SPAN , N-TAP) and related inspection engines	551
Configuring inspection engines	552
Configuring the Guardium portal	555
Configuring authentication	556
Enabling smart card authentication	557
Configuring multi-factor authentication	559
Managing the TLS version	561
Global profile	562
The alert message template	564
Configuring the alerter	567
Facility and priority of syslog messages	568
Anomaly Detection	568
Session Inference	569
Allow (approve) S-TAP connection to Guardium (S-TAP certification)	569
IP to Hostname Aliasing	569
Configure Permission to Socket connection	570
Managing access to Guardium	570
Understanding Roles	571
Access for default roles and applications	573
Managing roles and permissions	578
How to create a role with minimal access	579
Managing users	580
Managing Guardium credentials with CyberArk	582
Creating a user who can run GuardAPI commands	582
Importing users from LDAP	583
Data Security - User Hierarchy and Database Associations	585
How to define User Hierarchies	586
Central Management	587
Guardium Component Services	588
Implementing Central Management	590
Implementing Central Management in a New Installation	590
Registering Units	590
Unregistering a Managed Unit	591
Synchronizing Portal User Accounts	592
Implementing Central Management in an Existing Installation	593
Using Central Management Functions	593
Managing expiring certificates	594
Deployment health views	594
Configuring a central manager for the deployment health views	595
Deployment health topology and table views	596
Deployment health dashboard	598
Scenario: Troubleshooting overloaded systems using the deployment health topology view	601
Creating a cross-CM health view	601
Viewing cross-CM health view deployment health data	602
Managing patches on a cross-CM health view system	603
S-TAP and GIM dashboard	603

Create and manage S-TAP clusters	604
Enterprise load balancing	605
Enabling enterprise load balancing and associating an S-TAP with a central manager	605
Associating S-TAP with managed units for load balancing	606
Restarting (resynchronizing) S-TAPs for enterprise load balancing	607
Viewing the enterprise load balancing load map	607
Viewing an enterprise load balancing activity report	608
Enterprise load balancing configuration parameters	608
Deployment inventory	610
Resource deployment view	610
Monitoring managed units	610
Creating managed unit groups	612
Installing security policies on managed units	612
Central patch management	613
Distributing authentication configuration	613
Distributing configurations	613
Working with configuration profiles	614
Distribute custom tables	615
Central manager redundancy	615
Managing your Guardium system	618
Guardium Administration	618
Certificates	619
Installing an appliance certificate to avoid a browser SSL certificate challenge	620
Configuring Guardium-S-TAP communication using an SSL certificate	621
Identify expired certificates and certificates that will expire within six months	622
Managing certificates by using Venafi	622
Creating a Venafi instance	622
Configuring Venafi for GUI and Sniffer certificates	622
Configuring Venafi for GIM certificates	623
Restoring the Guardium Insights certificate	624
Alerts	625
How to create a real-time alert	625
Notifications	626
Predefined alerts	626
Custom Alerting Class Administration	627
System performance and monitoring	627
Unit utilization and inspection core performance	628
Buffer usage monitor report	628
Unit utilization and Unit utilization details reports	629
Performance issue: buffer usage process not running	630
Performance issue: analyzer queue overflow	631
Performance issue: logger queue overflow	631
Configuring unit utilization data processing	632
Self Monitoring	633
Monitoring with SNMP	635
Running Query Monitor	636
Services Status panel	636
Scheduling	637
Job dependencies	637
Viewing job history	638
Aliases	639
Dates and Timestamps	640
Building Time Periods	641
Cipher suites	642
Comments	643
Customer Uploads	643
Stream Guardium data to another application	646
Big Data Intelligence	646
Big Data Intelligence with data marts	646
Configure key pair authentication for GBDI file extraction	647
Big Data Intelligence with data streaming	647
Configure GBDI data streaming	648
Exporting and importing definitions	649
Remote loggers	652
Manage Custom Classes	652
GDPR readiness: Considerations when configuring Guardium	652
Groups	653
Groups overview	653
Using the group builder	654
Creating and editing groups	654
Viewing group membership and where groups are used	655
Populating groups	655
Importing from external datasources	656
Using groups in queries and policies	657
Example: Using groups to create rules and policies	657
Predefined Groups	658

Security Roles	662
How to install patches	663
Support Maintenance	664
Product integration	664
Configure BIG-IP Application Security Manager (ASM) to communicate with Guardium system	665
Embedded integrations	665
Integrating with IBM Knowledge Catalog for federated data protection	665
Starting the IBM Knowledge Catalog and Guardium Data Protection integration	667
Setting up a transformation integration	668
PIM integration	669
Configuring an external ticketing system	670
Configuring vulnerability scanner agents	672
QRadar and Guardium integration	672
OPTIM to Guardium Interface	674
Combining real-time alerts and correlation analysis with SIEM products	674
CEF Mapping	676
LEEF Mapping	677
Troubleshooting problems	678
Techniques for troubleshooting problems	679
Getting fixes from Fix Central	680
Contacting IBM Support	680
Basic information for IBM Support	681
Running must gather in the UI	681
Running must gather from the CLI	681
Running the slon looper utility	682
Configuring the slon looper utility	683
Must gather for UNIX-Linux S-TAP	683
Must gather for Windows S-TAP and other Windows agents	684
Running Must Gather V3.0	686
Exchanging information with IBM	686
Problems and solutions	687
User interface	687
Changes are not saved when you add an inspection engine	688
HTTP error 403	688
Java.lang.IllegalStateException	688
Pages are not loading correctly	689
Policies	689
Query does not appear in the co-relation alert definition	689
Rule does not trigger	690
REDACT function causes overly masked result	690
REDACT - Working with regex on Windows DB servers	691
SSH sessions and automated CRON jobs that log in to your Oracle database are shown as failed logins	692
Reports	692
Cannot modify the receiver table for an Audit Process after it has been executed at least once	693
Cannot see multi-byte characters	693
File system is almost full	693
Guardium audit reports viewed in Microsoft Excel have rows with unexpected characters	694
Reports show IP address as 0.0.0.0	694
Request was interrupted or quota exceeded error message	694
Scheduled Job Exceptions every 5 minutes	695
Scheduled jobs exception: merge required, delay executing process	696
The database user is not shown correctly in Guardium reports when you monitor Teradata	696
Unexpected results in Guardium reports with embedded commands	696
Assess and harden	697
CAS is not working with Java 1.7 on Windows	697
Vulnerability Assessment exception group members appear in failed test	697
Configuring your Guardium system	698
Cannot configure STAP after upgrade	698
Guardium fails to recognize the network device VMXNET x	699
Guardium network interface error after system board replacement	699
SSLv3 is enabled	699
Access management	700
Cannot log in to Guardium except as admin or accessmgr	700
Guardium accessmgr password reset	700
Guardium CLI password reset	701
Aggregation	701
Cannot convert Guardium collector to aggregator	702
Data Export configuration change from a Guardium managed system's GUI fails with error	702
Difference between audit process results and report	703
HY000 errors after restoring the configuration in an aggregator	703
UI banner warning: Data not exported or archived	704
Health alerts and UI banner warning: Old partitions found	704
Internal database	705

Why is the Guardium internal database is filling up	705
Managed unit database is filling up	706
How to purge off some old audit results from the Guardium appliance	706
Resolving internal database full problems	707
Central management	708
A user is disabled in a Guardium managed unit, but shows as enabled on Central Manager	708
Central Manager does not recognize the new version of upgraded units	709
Scheduled tasks do not fire at the scheduled time	709
Torque exception in Central Management view of GUI	710
S-TAPs and other agents	710
Error opening shared memory area when you configure Guardium COMM_EXIT_LIST for DB2	710
Guardium fails to collect shared memory traffic from Informix	711
High CPU and I/O Use in Guardium S-TAP host	711
UNIX S-TAP cannot start: buffer size too large	712
S-TAP does not start automatically on Linux	712
S-TAP returns not FIPS 140-2 compliant	713
The K-TAP kernel module is still present after the uninstallation of S-TAP	713
Windows S-TAP service crashes on startup with error ID 1000	714
S-TAP is not capturing A-TAP traffic	714
Linux S-TAP is not capturing Db2 exit traffic	715
Insufficient memory when installing UNIX S-TAP	715
Collectors	716
Nanny process is killing sniffer	716
Sniffer cannot connect to UNIX S-TAP	716
Guardium Installation Manager (GIM)	716
Error installing the Guardium Installation Manager (GIM)	717
Guardium Installation Manager (GIM) service does not start in Windows	717
File activity	717
File activity is not logged in investigation dashboard or reports	717
File activity from removable disk is not logged in investigation dashboard	718
File activity appears in reports but not the investigation dashboard	718
Some files missing from classification results	718
Partial file discovery (entitlement) results in reports and investigation dashboard	718
File classification results are missing from reports and investigation dashboard	719
File activity logs	719
FAM bundle fails to install	719
Investigation dashboard	720
Troubleshooting the investigation dashboard and enterprise search	720
Guardium installation	721
Checksum error during S-TAP installation	721
Guardium S-TAP returns an illegal cp: option - f error message	721
Installing a new Guardium patch does not complete	722
Missing file or directory after new Guardium S-TAP installation	722
Partition error installing Guardium	723
Patch installation fails: No such file or directory	724
z/OS	724
z/OS S-TAP fails to show active the Guardium system	724
Guardium universal connector	724
Overview	725
Configuring policies for Universal connector	725
Creating and managing secrets	726
Enabling universal connector on collectors	726
Adding connectors and plug-ins	727
Universal connector configuration	727
Creating credentials	728
Creating data source profiles	728
Creating Kafka clusters	729
Managing plug-ins	730
Configuring universal connectors	730
Monitoring connector and data flow status	731
Troubleshooting universal connectors	731
Troubleshooting tool	732
Logstash StackOverflow error due to large plug-in config file	732
Windows: S-TAP user's guide	734
Windows: S-TAP authentication guidelines	734
Windows: S-TAP protocol 8	734
Windows: Install, upgrade, and uninstall the S-TAP agent	735
Windows: Install S-TAP agents installation flow	735
Windows: S-TAP monitoring mechanisms support matrix	736
Windows: Auto discovery of database instances during installation and upgrade	736
Windows: Prerequisites: Installing S-TAP	736
Windows: S-TAP disk space requirements	736
Windows: Guardium port requirements for S-TAP	737
Windows: Use GIM to install, upgrade, uninstall the S-TAP	737

Windows: Installing S-TAP agent with GIM Setup by Client	737
Windows: S-TAP GIM installation parameters	738
Windows: Upgrading S-TAP agent with GIM Setup by Client	739
Windows: Uninstalling an S-TAP agent with GIM Set up by Client	740
Windows: Use interactive installer (wizard) to install, upgrade, uninstall the S-TAP	740
Windows: Installing S-TAP agent by using the interactive installer	741
Windows: Upgrading the S-TAP agent using the interactive installer	741
Windows: Use CLI to install, upgrade, uninstall the S-TAP	742
Windows: Installing S-TAP agent using the command line interface	742
Windows: S-TAP command line installation parameters	743
Windows: Upgrading S-TAP using the command line	744
Windows: Uninstalling S-TAP using the command line	744
Windows: Remove the S-TAP using Add/Remove Programs	745
Windows: S-TAP installation flow on Oracle RAC	745
Windows: Managing S-TAP when upgrading your database	745
Windows: Managing S-TAP when upgrading your database operating system	745
Windows: When to restart or reboot the database server after installing or upgrading S-TAP	746
Windows: Managing S-TAP when upgrading your database	745
Windows: Managing S-TAP when upgrading your database operating system	745
Windows: Configuring S-TAP	747
Windows: Configuring S-TAP in the S-TAP Control page	747
S-TAP Control: Details	749
S-TAP Control: Change auditing	750
S-TAP Control: Application server user identification	750
S-TAP Control: Guardium Hosts	751
S-TAP Control: Firewall Details	751
S-TAP Control: Inspection Engines	751
Windows: Configuring S-TAP with guard_config_update	753
Windows: Discover database instances	754
Windows: Configuring an Inspection Engine	754
Windows: Inspection engine verification	755
Windows: S-TAP verification	755
Windows: Configure standard verification	756
Windows: Configure advanced verification	756
Windows: Configuring the S-TAP verification schedule	756
Windows: S-TAP load balancing models and configuration guidelines	757
Windows: Configuring the Db2 Exit library	758
Windows: Upload dump files from the S-TAP to the collector and central manager	759
Windows: Build and configure FreeTDS for Guardium	759
Windows: S-TAP configuration per database type	760
Windows: Db2 configuration for SSL	760
Windows: S-TAP operation and performance	760
Windows: Stopping S-TAP using GIM	761
Windows: Starting S-TAP using GIM	761
Windows: Starting S-TAP without GIM	761
Windows: Stopping S-TAP without GIM	762
Windows: Multi-threading S-TAP for increased throughput	762
Windows: Capturing encrypted MSSQL traffic	763
Windows: Alerts on uninstalled S-TAPs	764
Windows: Deleting inactive S-TAPs in a centralized environment	764
Windows: Monitoring S-TAP in the GUI	764
Windows: Log and debug files	765
Windows: S-TAP statistics	766
Windows: Monitoring with the Guardium Agent Monitor	766
Windows: Troubleshooting S-TAP problems	769
Windows: Scheduling S-TAP diagnostics	770
Linux-UNIX: S-TAP user's guide	770
Linux-UNIX: S-TAP functionality	770
Linux-UNIX: S-TAP monitoring mechanisms support matrix	770
Linux-UNIX: S-TAP monitoring mechanisms	771
Linux-UNIX: S-TAP to collector encryption	771
Linux-UNIX: UID chains	772
Linux-UNIX: Proxy firewall	773
Linux-UNIX: Using automation tools with the S-TAP and sample scripts	773
Linux-UNIX: Installing, upgrading and uninstalling S-TAP agents	776
Linux-UNIX: Install S-TAP agents installation flow	776
Linux-UNIX: S-TAP installation prerequisites	777
Linux-UNIX: Database version and directory requirements	777
Linux-UNIX: Disk space requirements for S-TAP	777
Linux-UNIX: Port requirements for S-TAP	778
Linux-UNIX: System details and checks	778
Linux-UNIX: Before you start installing S-TAP	778
Linux-UNIX: Use GIM to install, upgrade, uninstall the S-TAP	779
Linux-UNIX: Installing the S-TAP client with GIM Setup by Client	779
Linux-UNIX: S-TAP GIM installation parameters	780
Linux-UNIX: Upgrading an S-TAP agent with GIM Setup by Client	781

Linux-UNIX: Uninstalling S-TAP agent with GIM Setup by Client	782
Linux-UNIX: Use RPM to install, upgrade, uninstall the S-TAP	783
Linux-UNIX: Installing the S-TAP agent with RPM	783
Linux-UNIX: S-TAP guard-config-update parameters for RPM installation and update	784
Linux-UNIX: Upgrading S-TAP using RPM	787
Linux-UNIX: Uninstalling S-TAP using RPM	788
Linux-UNIX: Use shell installer to install, upgrade, uninstall the S-TAP	788
Linux-UNIX: Installing the S-TAP client by using the shell installer	788
Linux-UNIX: S-TAP install script parameters	789
Linux-UNIX: Upgrading the S-TAP agent using the shell installer	790
Linux-UNIX: Uninstalling S-TAP agents using the shell installer	791
Linux-UNIX: Converting a shell managed S-TAP to a GIM managed S-TAP	791
Linux-UNIX: Use native installers to install, upgrade, uninstall the S-TAP	792
Linux-UNIX: Installing and uninstalling S-TAP with AIX native installer	792
Linux-UNIX: Installing and uninstalling S-TAP with HP-UX native installer	793
Linux-UNIX: Installing and uninstalling the S-TAP with Solaris native installer	793
Linux-UNIX: S-TAP upgrade workflows per monitoring mechanism	794
Linux-UNIX: Upgrading S-TAP with databases that use A-TAP	794
Linux-UNIX: Upgrading S-TAP with databases that use an exit library	794
Linux-UNIX: Working with K-TAP	796
Linux-UNIX: Preparing to install K-TAP	796
Linux-UNIX: S-TAP compilation of K-TAP	797
Linux-UNIX: Enrolling a K-TAP signing key	797
Linux-UNIX: Signing and enrolling a locally built K-TAP	798
Linux-UNIX: Copying a K-TAP module with GIM	799
Linux-UNIX: Copying a K-TAP module from the command line	800
Linux-UNIX: Enable K-TAP after installation if P-CAP was installed by default	800
Linux-UNIX: Requesting a K-TAP module	800
Linux-UNIX: K-TAP FAQs	802
Linux-UNIX: Special environments configuration	802
Linux-UNIX: Solaris Zones configuration	802
Linux-UNIX: Oracle RAC S-TAP configuration	804
Linux-UNIX: Configure S-TAP for Db2 WPAR	806
Linux-UNIX: Configure S-TAP for SELinux	807
Linux-UNIX: Activating and deactivating A-TAP on all nodes of a Db2 Cluster	807
Linux-UNIX: Configure delayed cluster disk mounting	808
Linux-UNIX: What to restart or reboot on the database server after installing or updating S-TAP	809
Linux-UNIX: Managing a GIM-, RPM-, and shell-installed S-TAP during a database upgrade	809
Linux-UNIX: Managing GIM clients during a major upgrade of the database server operating system	810
Linux-UNIX: Managing an RPM- or shell-installed S-TAP during a major upgrade of the database server operating system	810
Linux-UNIX: Managing a GIM-, RPM-, or shell-installed S-TAP during a minor or kernel upgrade of the database server operating system	811
Linux-UNIX: Configuring S-TAP	812
Linux-UNIX: Configuring S-TAP in the S-TAP Control page	812
Linux-UNIX: S-TAP Control: Details	814
Linux-UNIX: S-TAP Control: Change auditing parameters	817
Linux-UNIX: S-TAP Control: Application server user identification parameters	817
Linux-UNIX: S-TAP Control: Guardium Hosts parameters	818
Linux-UNIX: S-TAP Control: Firewall parameters	818
Linux-UNIX: S-TAP Control: Inspection engine parameters	818
Linux-UNIX: Scheduling S-TAP diagnostics	820
Linux-UNIX: Configure S-TAP with guard-config-update	820
Linux-UNIX: Discover database instances	821
Linux-UNIX: Configuring an Inspection Engine	822
Linux-UNIX: Inspection engine verification	823
Linux-UNIX: S-TAP verification	823
Linux-UNIX: Configure standard verification	824
Linux-UNIX: Configure advanced verification	824
Linux-UNIX: Configuring the S-TAP verification schedule	825
Linux-UNIX: S-TAP load-balancing models and configuration guidelines	825
Linux-UNIX: Kerberos-authenticated database traffic	826
Linux-UNIX: Kerberos authentication supported databases	827
Linux-UNIX: Configuring Kerberos by using the setup_kerberos.sh script	827
Linux-UNIX: Enabling the Kerberos plugin	828
Linux-UNIX: Configuring the Kerberos plugin	828
Linux-UNIX: Finding the Kerberos configuration parameters for Oracle	829
Linux-UNIX: Finding the Kerberos configuration parameters for Sybase	829
Linux-UNIX: Merging keytab files	829
Linux-UNIX: A-TAP management	830
Linux-UNIX: Preparing for A-TAP configuration and maintenance	831
Linux-UNIX: A-TAP configuration and activation	831
Linux-UNIX: A-TAP activate, deactivate and DB stop, restart guidelines	832
Linux-UNIX: guardctl utility commands for A-TAP	832
Linux-UNIX: guardctl return codes	834
Linux-UNIX: Database-specific guardctl parameters	835

Linux-UNIX: Db2-specific guardctl parameters	835
Linux-UNIX: Informix-specific guardctl parameters	836
Linux-UNIX: Greenplum-specific guardctl parameters	836
Linux-UNIX: Mongo-specific guardctl parameters	836
Linux-UNIX: Oracle-specific guardctl parameters	837
Linux-UNIX: Postgres-specific guardctl parameters	837
Linux-UNIX: Sybase-specific guardctl parameters	838
Linux-UNIX: Sybase IQ-specific guardctl parameters	839
Linux-UNIX: Teradata-specific guardctl parameters	839
Linux-UNIX: Vertica-specific guardctl parameters	840
Linux-UNIX: Deactivating A-TAP	840
Linux-UNIX: Configuring and Activating A-TAP in Special Environments	841
Linux-UNIX: Activating A-TAP for Oracle on a Veritas Cluster	841
Linux-UNIX: Installing and activating A-TAP in Solaris zones	841
Linux-UNIX: Installing and activating A-TAP in WPARs environment	843
Linux-UNIX: Deactivate and uninstall A-TAP in Zones and WPARs environment	843
Linux-UNIX: Upgrading A-TAP in Zones and WPARs environment	844
Linux-UNIX: Configure and activate A-TAP steps for Teradata database	845
Linux-UNIX: Oracle considerations for A-TAP	846
Linux-UNIX: Troubleshooting A-TAP configuration issues	846
Linux-UNIX: Configure a public and private address for an S-TAP	847
Linux-UNIX: Configure S-TAP log and dump locations when /root partition size is limited	847
Linux-UNIX: Editing the S-TAP configuration parameters	848
Linux-UNIX: Guardium Hosts (SQLGuard) parameters	849
Linux-UNIX: General parameters	849
Linux-UNIX: Inspection engine parameters	855
Linux-UNIX: Oracle Unified Auditing parameters	857
Linux-UNIX: Firewall parameters	857
Linux-UNIX: Query rewrite parameters	858
Linux-UNIX: Server-side masking (SSM) parameters	858
Linux-UNIX: Discovery parameters	859
Linux-UNIX: Application server parameters	859
Linux-UNIX: Hadoop parameters	860
Linux-UNIX: Configuration Auditing System (CAS) parameters	862
Linux-UNIX: Debug parameters	862
Linux-UNIX: K-TAP parameters	863
Linux-UNIX: S-TAP configuration per database type	864
Linux-UNIX: Configuring Apache Cassandra and S-TAP for auditing interception	865
Linux-UNIX: Application server S-TAP configuration	866
Linux-UNIX: CockroachDB inspection engine configuration	867
Linux-UNIX: Couchbase auditing configuration	867
Linux-UNIX: Using SAP-HANA with encrypted connections	870
Linux-UNIX: Datastax Cassandra auditing configuration	871
Linux-UNIX: Db2 IE configuration	872
Linux-UNIX: Elastic Search configuration	873
Linux-UNIX: Configuring Exit libraries	874
Linux-UNIX: Configuring Db2, Informix, and Teradata exit by using the setup_exit.sh script	874
Linux-UNIX: Configuring Db2 Exit	875
Linux-UNIX: Configuring Informix Exit	876
Linux-UNIX: Configuring Teradata exit	877
Linux-UNIX: Disabling Teradata exit	880
Linux-UNIX: Hadoop configuration	881
Linux-UNIX: Hadoop integration with Ranger HDFS for Hortonworks and Cloudera 7	881
Linux-UNIX: Configuring S-TAPs: Ranger HDFS for Hortonworks and Cloudera 7	882
Linux-UNIX: Upgrading and uninstalling S-TAPs: Ranger HDFS for Hortonworks and Cloudera 7	883
Linux-UNIX: Ranger HDFS for Hortonworks and Cloudera 7 FAQs	883
Linux-UNIX: Hadoop integration with Cloudera Navigator	883
Linux-UNIX: Planning the integration with Cloudera Navigator	885
Linux-UNIX: Preliminary configuration	885
Linux-UNIX: Configure publication of Navigator audit events to Kafka	886
Linux-UNIX: Configuring the S-TAP for Cloudera	886
Linux-UNIX: Validate and troubleshoot the Cloudera configuration	887
Linux-UNIX: Hadoop integration using Hortonworks and Apache Ranger	887
Linux-UNIX: Hortonworks Ranger architecture and data flow	888
Linux-UNIX: Planning the integration with Hortonworks and Apache Ranger	889
Linux-UNIX: Hortonworks and Apache Ranger prerequisites	889
Linux-UNIX: FAQs Hortonworks Ranger configuration	890
Linux-UNIX: Configure the solution for monitoring	890
Linux-UNIX: Configure the Ranger plugins using Ambari	890
Linux-UNIX: Configure Guardium and Ranger communication	891
Linux-UNIX: Install and configure S-TAPs	892
Linux-UNIX: MongoDB IE configuration	893
Linux-UNIX: Neo4J auditing configuration	893

Linux-UNIX: Oracle Connection Manager configuration to monitor encrypted traffic	896
Linux-UNIX: Install and configure the Oracle Connection Manager on the database server	896
Linux-UNIX: Install and configure the Oracle Connection Manager in an Oracle RAC environment	897
Linux-UNIX: Install and configure the Oracle Connection Manager on a remote server	898
Linux-UNIX: Oracle IE configuration	899
Linux-UNIX: Configuring S-TAP interception using Oracle Unified Audit	900
Linux-UNIX: Redis configuration	901
Linux-UNIX: S-TAP operation and performance	902
Linux-UNIX: Stopping S-TAP using GIM	902
Linux-UNIX: Starting S-TAP using GIM	903
Linux-UNIX: Start and stop S-TAP and GIM processes for various OS types/versions	903
Linux-UNIX: Start and stop methods for inittab	903
Linux-UNIX: Start and stop methods for Solaris services	904
Linux-UNIX: Start and stop methods for systemd	904
Linux-UNIX: Start and stop methods for upstart	904
Linux-UNIX: Using guard-config-update to start, restart, and stop S-TAP, and view status	904
Linux-UNIX: Optimizing your configuration for high load	905
Linux-UNIX: Multi-threading S-TAP to increase S-TAP throughput	905
Linux-UNIX: Increasing S-TAP and K-TAP throughput with dynamic ring buffers	909
Linux-UNIX: Alerts on uninstalled S-TAPs	909
Linux-UNIX: Deleting inactive S-TAPs in a centralized environment	910
Linux-UNIX: Monitoring S-TAP in the GUI	910
Linux-UNIX: S-TAP logs	911
Linux-UNIX: Viewing S-TAP debug details on the database	911
Linux-UNIX: Determine the S-TAP version	911
Linux-UNIX: S-TAP statistics	911
Linux-UNIX: S-TAP Monitor (guard_monitor)	914
Linux-UNIX: Troubleshooting S-TAP problems	917
Db2 for IBM i S-TAP	918
Monitoring strategy	919
Installing the S-TAP for IBM i	920
Uninstalling the S-TAP	921
Upgrading the S-TAP from 10.x to 11.x for IBM i	921
Defining the S-TAP for IBM i	922
External S-TAP	923
External S-TAP requirements	925
SSL certificates for External S-TAP	926
Configure on-demand certificate generation	927
Manually create a certificate signing request	927
Verify collector certificates (optional)	928
Verifying client and server certificates	929
Importing a custom certificate	929
Configuring mutual authentication	930
Configuring certificate mirroring	930
Preparing SSL certificates for client applications	932
Deploying External S-TAP with an operator	933
Mirroring images to your private container registry	934
Configuring the cluster to pull images	936
Creating catalog sources	937
Creating operator subscriptions	937
Enabling the External S-TAP provisioning UI	938
Provisioning an instance of External S-TAP	939
Deploying External S-TAP with Helm	941
Deploying External S-TAP from the Guardium UI	942
Deploying External S-TAP manually	943
Download the Docker container	943
External S-TAP deployment scripts	944
Load balancer scripts	947
The External S-TAP user interface	948
Deploy External S-TAP window	949
Kubernetes tab	949
Volume tab	950
Docker tab	950
Database tab	950
Guardium tab	950
Certificate tab	951
Advanced tab	951
Edit External S-TAP group tab	951
TAP tab	952
Inspection engine tab	953
Collector tab	953
Firewall tab	953
Best practices for using External S-TAPs with on-premises databases	954
Configuring AWS HA for External S-TAPs	955
Configuring Google BigQuery for External S-TAPs	956
Troubleshooting External S-TAP issues	957

Guardium Installation Manager	959
GIM management	959
Creating and managing custom GIM certificates	959
Replacing default GIM certificate with SHA1 or SHA256 certificate	961
GIM server failover	961
Running GIM diagnostics	962
Enable/disable the GIM server log	962
GIM server allocation	962
Install, upgrade, and uninstall GIM clients on Linux-UNIX servers	964
Installing the GIM client on a UNIX server	964
Upgrading the GIM client	966
Uninstalling GIM and its modules on a UNIX database	966
Installing GIM and other packages on Linux servers by using the consolidated installer	966
Managing GIM clients during a major upgrade of the database server operating system	967
Install, upgrade, and uninstall GIM clients on Windows servers	968
Installing the GIM client on a Windows server	968
Installing GIM and other packages on Windows servers by using the consolidated installer	969
Starting and stopping the GIM client on a Windows server	970
Managing GIM clients	970
GIM global parameters	970
Using groups with GIM	971
GIM dynamic updating	972
Managing software with GIM	972
Deploy monitoring agents	972
Set up by Client	974
Uploading and importing GIM modules	975
Centralized module view	976
Managing bundles by using the configurator.sh script	976
GIM CLI commands	977
GIM user interfaces	979
Distributing GIM bundles to managed units	980
Removing unused GIM bundles	980
Starting and restarting GIM services and components	981
Restarting the supervisor for Solaris with SMF support	981
Installing your Guardium system	981
Operating modes	982
License keys	982
Hardware Requirements	983
Guardium port requirements	983
Step 1. Assemble the following before you begin	986
SAN storage devices	986
Step 2. Set up the physical or virtual appliance	986
Physical Appliance	986
Identify network ports	986
Default passwords for physical appliances	987
Virtual appliance	987
Step 3. Install the Guardium image	987
Step 4. Set up initial and basic configuration	988
Set the primary and secondary system IP addresses	988
Set the Default Router IP Address	988
Set DNS Server IP Address	989
SMTP Server	989
Set Host and Domain Names	989
Set the Time Zone, Date and Time	989
Set the Initial Unit Type	989
Resetting the root password	990
Validate All Settings	990
Reboot the System	990
Step 5. What to do next	990
Verify Successful Installation	991
Set Unit Type	991
Install license keys	991
Install maintenance patches (if available)	992
Additional Steps (optional)	992
Creating the Virtual Image	993
VMware Infrastructure Overview	993
VM Installation Overview	994
Creating a Hyper-V Virtual Machine	996
Red Hat Virtualization	997
vMotion Installation	998
Custom Partitioning	998
How to partition with an encrypted LVM	999
Create an LVM disk with four disks	999
Example of SAN Configuration	1000
Upgrading your Guardium system	1002
Planning an upgrade	1002
Identifying the correct upgrade path	1002
Mixed-version environments during an upgrade	1003

Upgrading with central managers and aggregators	1004
Upgrading an environment with a central manager	1004
Preparing for upgrade	1004
Upgrading the central manager	1005
Applying the health check patch	1005
Archiving data	1005
Purging system data	1006
Backing up the system	1006
Applying the upgrade patch	1007
Installing maintenance patches	1007
Upgrading the managed unit	1007
Applying the health check patch	1008
Archiving data	1008
Purging system data	1009
Backing up the system	1009
Applying the upgrade patch	1009
Installing maintenance patches	1010
Upgrading S-TAP agents	1010
Upgrading a stand-alone system	1010
Preparing for upgrade	1011
Applying the health check patch	1011
Archiving data	1011
Purging system data	1012
Backing up the system	1012
Applying the upgrade patch	1013
Installing maintenance patches	1013
Upgrading S-TAP agents	1013
Deploying Guardium on a cloud service	1014
CLI Commands	1014
Using the CLI	1014
Aggregator CLI Commands	1016
Alerter CLI Commands	1019
Certificate CLI Commands	1022
Configuration and control CLI commands	1029
diag CLI command	1059
File handling CLI Commands	1069
Inspection Engine CLI Commands	1076
Investigation Dashboard CLI Commands	1079
Network Configuration CLI Commands	1079
Support CLI Commands	1084
System CLI Commands	1098
User account, password, and authentication CLI Commands	1109
GuardAPI and REST API commands	1114
Using GuardAPI commands	1116
Using Guardium REST APIs	1119
Guardium API A-Z Reference	1121
add_action_to_fam_rule	1133
add_all_to_schedule	1134
add_approved_stap_client	1135
add_assessment_datasource	1135
add_assessment_datasource_group	1136
add_assessment_test	1136
add_assessment_test_by_dsId	1137
add_autodetect_task	1138
add_available_test_notes	1138
add_classifier_datasource	1139
add_classifier_datasource_group	1139
add_cluster	1139
add_connection_properties	1140
add_custom_property_to_datasource_by_id	1141
add_custom_property_to_datasource_by_name	1141
add_custom_property_to_datasources_in_group	1142
add_datasource_to_entitlement_optimization	1142
add_datasource_to_group	1144
add_dm_to_profile	1144
add_domain_to_universal_connector_allowed_domains	1145
add_group_to_quick_search	1146
add_ip_to_sg	1147
add_mfa_exempt_users	1147
add_objects_native_audit	1148
add_ranger_config	1149
add_ranger_hdfs_config	1150
add_ranger_service	1151
add_receiver_to_rule_action	1152
add_stream	1153
add_threshold_to_rule	1154

add_time_period	1155
aggregation	1156
apply_rules_on_discoveredinstances	1156
assign_analytic_case	1157
assign_collectors	1158
assign_load_balancer_groups	1159
assign_qr_condition_to_action	1160
audit_process_run_status	1161
auto_execute_suggested_dependencies	1161
backup_cm_list_candidates	1162
backup_cm_set	1162
cancel_distributed_report_target	1163
change_cli_password	1163
change_monitor_value	1164
change_rule_order	1165
change_to_microsoft	1165
change_to_opensource	1166
change_tracker_get_events	1166
change_tracker_get_params	1167
change_tracker_get_tasks	1168
change_tracker_reset	1169
change_tracker_set_params	1170
clear_cas_template_set	1171
clevis_bind	1171
clone_assessment	1172
clone_cas_template_set	1172
clone_extraction_profile	1173
clone_policy	1174
close_default_events	1174
configure_archive	1175
configure_data_streaming	1176
configure_export	1177
configure_mfa	1178
configure_purge	1179
configure_results_archive	1180
configure_results_export	1182
configure_system_backup	1183
copy_key_file	1184
copy_rule	1184
copy_rules	1185
create_ad_hoc_audit_and_run_once	1186
create_ad_hoc_audit_and_run_with_name	1187
create_ad_hoc_audit_for_security_assessment	1188
create_adhoc_policy_analyzer	1189
create_alias	1189
create_allowed_db	1190
create_api_key	1191
create_api_parameter_mapping	1191
create_assessment	1192
create_autodetect_process	1192
create_aws_secrets_manager_config	1193
create_cas_host_instance	1194
create_cas_template	1194
create_cas_template_set	1195
create_classifier_action	1196
create_classifier_document_rule	1197
create_classifier_policy	1198
create_classifier_process	1199
create_classifier_rule	1199
create_cloudTitle	1201
create_cloud_datasource	1202
create_computed_attribute	1203
create_constant_attribute	1204
create_custom_table_ldap_import	1205
create_cyberark_config	1206
create_datasource	1206
create_datasourceRef_by_id	1208
create_datasourceRef_by_name	1209
create_datasource_custom_property	1209
create_datasource_group	1210
create_datasource_groupRef_by_id	1210
create_datasource_groupRef_by_name	1210
create_db_user_mapping	1211
create_ef_mapping	1212
create_entry_location	1212
create_fam_rule	1213
create_group	1215
create_hashicorp_config	1216
create_hierarchical_member_to_group_by_desc	1216
create_kafka_cluster	1217

create_member_to_group_DAMX_Standard_Activity	1217
create_member_to_group_DAMX_Suspicious_Connections	1217
create_member_to_group_by_desc	1217
create_member_to_group_by_id	1218
create_online_report	1218
create_policy	1219
create_qr_action	1220
create_qr_add_where	1221
create_qr_add_where_by_id	1221
create_qr_condition	1222
create_qr_definition	1223
create_qr_replace_element	1224
create_qr_replace_element_byId	1224
create_quarantine_allowed_until	1225
create_quarantine_until	1226
create_role	1227
create_rule	1227
create_rule_action	1228
create_sql_configuration	1228
create_stap_inspection_engine	1229
create_test_detail_exception	1231
create_test_exception	1232
create_update_wkc_config	1233
create_user	1234
create_user_hierarchy	1235
datamart_copy_file_bundle	1235
datamart_include_file_header	1236
datamart_refresh_metadata	1237
datamart_run_once_now	1237
datamart_set_active	1238
datamart_set_date_format	1238
datamart_set_inactive	1239
datamart_update_copy_file_info	1239
datamart_validate_copy_file_info	1240
delete_adhoc_policy_analyzer	1241
delete_alerter_snmp_settings	1242
delete_alias	1242
delete_allowed_db_by_entry_id	1242
delete_allowed_db_by_user	1243
delete_analytic_user_feedback	1244
delete_api_parameter_mapping	1244
delete_approved_stap_client	1245
delete_archive_configuration	1245
delete_assessment	1246
delete_assessment_datasource	1247
delete_assessment_datasource_group	1247
delete_assessment_test	1247
delete_audit_process	1248
delete_audit_process_result	1248
delete_autodetect_process	1249
delete_autodetect_scans_for_process	1250
delete_available_test_notes	1250
delete_aws_secrets_manager_config	1251
delete_cas_host	1251
delete_cas_host_instance	1252
delete_cas_template	1252
delete_cas_template_set	1253
delete_classifier_action	1253
delete_classifier_document_rule	1254
delete_classifier_policy	1254
delete_classifier_process	1255
delete_classifier_rule	1255
delete_cluster	1255
delete_computed_attribute	1256
delete_constant_attribute	1256
delete_cust_table_distribution_schedule	1257
delete_custom_table_ldap_import	1258
delete_cyberark_config	1258
delete_datasourceRef_by_id	1259
delete_datasourceRef_by_name	1259
delete_datasource_by_id	1260
delete_datasource_by_name	1261
delete_datasource_configuration	1261
delete_datasource_custom_property	1262
delete_datasource_group	1262
delete_datasource_groupRef_by_id	1263
delete_datasource_groupRef_by_name	1263
delete_db_user_mapping	1263
delete_distributed_report_result_for_period	1264
delete_ef_mapping	1265

delete_entry_location	1265
delete_export_configuration	1266
delete_group_by_desc	1267
delete_group_by_id	1267
delete_group_from_quick_search	1268
delete_hashicorp_config	1269
delete_hierarchical_member_from_group_by_desc	1269
delete_imscheckpoint_record	1270
delete_inactive_stap	1270
delete_invalid_stap	1271
delete_kafka_cluster	1272
delete_member_from_group_by_desc	1272
delete_member_from_group_by_id	1272
delete_oauth_clients	1273
delete_policy	1273
delete_quarantine	1274
delete_ranger_hdfs_config	1275
delete_results_archive_configuration	1276
delete_results_export_configuration	1276
delete_rule	1277
delete_schedule	1277
delete_sql_configuration	1278
delete_stap_inspection_engine	1279
delete_stream	1280
delete_system_backup_configuration	1280
delete_test_detail_exception	1281
delete_test_detail_exception_by_id	1281
delete_test_exception	1282
delete_test_exception_by_id	1282
delete_user	1283
delete_user_hierarchy_by_entry_id	1283
delete_user_hierarchy_by_user	1284
disable_advanced_threat_scanning	1284
disable_auto_execute_suggested_dependencies	1285
disable_big_data_interface	1286
disable_datastream	1287
disable_embed_eastern_font	1287
disable_entitlement_optimization	1287
disable_fam_crawler	1288
disable_health_analyzer	1289
disable_ip_to_host_aliases	1289
disable_monitoring_ranger_service	1290
disable_native_audit	1291
disable_outliers_detection	1291
disable_outliers_detection_agg	1292
disable_outliers_detection_cross_cm_agg	1293
disable_outliers_detection_cross_cm_collector	1293
disable_persistent_queue_universal_connector	1294
disable_policy_analyzer	1295
disable_purge	1295
disable_quick_search	1296
disable_riskspotter	1297
disable_special_attributes	1297
disable_test_result_detail_string_setting	1298
disable_threat_detection_use_case	1298
disable_threat_finder	1299
discover_streams	1300
display_external_stap_config	1301
display_stap_config	1303
edit_kafka_cluster	1309
enable_advanced_threat_scanning	1310
enable_all_tls	1310
enable_big_data_interface	1311
enable_datastream	1312
enable_disable_ip_restriction	1313
enable_disable_monitoring_streams	1313
enable_embed_eastern_font	1315
enable_entitlement_optimization	1315
enable_fam_crawler	1316
enable_fips_tls	1317
enable_health_analyzer	1318
enable_health_traffic_job	1318
enable_ip_to_host_aliases	1319
enable_latest_tls	1319
enable_monitoring_ranger_service	1320
enable_native_audit	1322
enable_outliers_detection	1322
enable_outliers_detection_agg	1324
enable_outliers_detection_cross_cm_agg	1325
enable_outliers_detection_cross_cm_collector	1326

enable_persistent_queue_universal_connector	1326
enable_policy_analyzer	1327
enable_quick_search	1328
enable_riskspotter	1328
enable_special_attributes	1329
enable_strong_cli_password	1330
enable_threat_detection_use_case	1330
enable_threat_finder	1331
encrypt_value	1332
execute_appUserTranslation	1332
execute_assessment	1333
execute_auditProcess	1333
execute_autodetect_process	1334
execute_cls_process	1335
execute_flatLogProcess	1336
execute_incidentGenProcess	1336
execute_incidentGenProcess_byDetails	1337
execute_ldap_user_import	1338
execute_populateGroupFromQuery	1338
export_certificate	1339
export_config	1340
export_definition	1340
export_log_files	1341
export_transfer_key	1342
f5_add_apps_config	1342
f5_add_data_params	1343
f5_delete_apps_config	1343
f5_delete_data_params	1343
f5_list_apps_config	1343
f5_list_data_params	1344
f5_update_data_params	1344
fipsmode	1344
flatten_hierarchical_groups	1345
generate_ssl_key_universal_connector	1345
generate_transfer_key	1346
getFieldsTitles	1346
getOAuthTokenExpirationTime	1347
get_all_modifiable_guard_params	1347
get_assessment_result	1348
get_cluster_members	1348
get_clusters	1349
get_datamart_info	1349
get_datasource_custom_properties	1350
get_debug_level	1351
get_definitions_data_sets	1351
get_definitions_items	1352
get_distributed_report_target_info	1352
get_entitlement_optimization_info	1352
get_expiration_date_for_restored_day	1353
get_extraction_profile_info	1354
get_fam_crawler_info	1355
get_flatLogProcessType	1355
get_guard_param	1356
get_hadoop_cluster_status	1356
get_health_traffic_status	1357
get_inapplicable_test_result_status	1357
get_insights_agent_config	1358
get_ip_restriction_config	1358
get_ip_to_alias_overwrites	1359
get_ip_to_alias_selected	1359
get_istap_config	1360
get_istap_status	1360
get_job_process_concurrency_limit	1361
get_kafka_clusters	1361
get_load_balancer_load_map	1361
get_load_balancer_params	1362
get_mfa_configuration	1362
get_native_audit_collectors	1363
get_native_audit_configurations	1363
get_native_audit_objects	1364
get_outliers_detection_info	1365
get_policy_analyzer_status	1366
get_purge_batch_size	1366
get_quick_search_info	1367
get_ranger_config	1368
get_ranger_hdfs_config	1369
get_ranger_services_status	1369
get_registered_units	1371
get_secured_protocols_info	1371
get_solr_cluster_info	1372

get_solr_errors	1372
get_solr_status	1373
get_solr_status_extended	1374
get_streams	1374
get_test_result_detail_string_setting	1375
get_threat_detection_use_case_info	1376
get_unit_data	1376
get_unit_pinger	1377
get_universal_connector_allowed_domains	1377
get_universal_connector_status	1378
get_va_summary_key	1379
get_wki_config	1379
get_ztap_logging_config	1379
gim_assign_bundle_or_module_to_client_by_version	1380
gim_assign_latest_bundle_or_module_to_client	1380
gim_cancel_install	1381
gim_cancel_uninstall	1381
gim_get_available_modules	1382
gim_get_client_last_event	1382
gim_get_global_param	1383
gim_get_modules_running_status	1384
gim_list_bundles	1384
gim_list_client_modules	1385
gim_list_client_params	1385
gim_list_mandatory_params	1386
gim_list_registered_clients	1386
gim_list_unused_bundles	1386
gim_load_package	1387
gim_remote_activation	1388
gim_remove_bundle	1388
gim_reset_client	1389
gim_schedule_install	1389
gim_schedule_uninstall	1390
gim_set_diagnostics	1391
gim_set_global_param	1391
gim_unassign_client_module	1392
gim_uninstall_module	1393
gim_update_client_params	1393
grant_role_to_object_by_Name	1394
grant_role_to_object_by_id	1394
health_info	1395
import_definitions	1395
insights_registration	1396
insights_unregistration	1396
kill_running_process	1396
list_adhoc_policy_analyzer	1397
list_aliases	1397
list_all_reports	1399
list_allowed_db_by_user	1408
list_api_key	1409
list_approved_stap_client	1409
list_assessment_tests	1409
list_assessments	1410
list_associated_stap_mu_groups	1410
list_audit_processes	1411
list_autodetect_processes	1412
list_autodetect_tasks_for_process	1412
list_available_test_notes	1413
list_available_tests	1413
list_aws_secrets_manager_config	1414
list_cas_host_instances	1414
list_cas_hosts	1415
list_cas_template_sets	1416
list_cas_templates	1417
list_classifier_policy	1418
list_classifier_process	1418
list_cloud_datasource_by_name	1419
list_compatibility_modes	1419
list_computed_attribute	1420
list_custom_table_ldap_imports	1421
list_cyberark_config	1421
list_datasourceRef_by_id	1421
list_datasourceRef_by_name	1422
list_datasource_by_id	1423
list_datasource_by_name	1423
list_datasource_groupRef_by_id	1424
list_datasource_groupRef_by_name	1424
list_datasource_group_hierarchy	1425
list_datasource_group_members	1425
list_datasource_groups	1425

list_db_drivers	1426
list_db_drivers_by_details	1426
list_db_user_mapping	1427
list_ef_mapping	1427
list_ef_report	1428
list_engine_config	1428
list_entry_location	1429
list_existing_job_dependencies	1430
list_expiration_dates_for_restored_days	1431
list_group_by_desc	1432
list_group_by_id	1432
list_group_members_by_desc	1433
list_group_members_by_id	1433
list_groups	1434
list_hashicorp_config	1435
list_health_node	1435
list_imscheckpoint_records	1436
list_inspection_engines	1436
list_installed_policies	1437
list_managed_units	1438
list_members_of_groups_by_desc	1439
list_members_of_groups_by_id	1439
list_oauth_clients	1440
list_param_mapping_for_function	1440
list_parameter_names_by_report_name	1441
list_policy	1441
list_policy_fam_rule	1442
list_policy_rules	1442
list_qr_action	1443
list_qr_add_where	1444
list_qr_add_where_by_id	1444
list_qr_condition	1445
list_qr_condition_to_action	1445
list_qr_definitions	1446
list_qr_replace_element	1447
list_qr_replace_element_byId	1448
list_quick_search_groups	1448
list_ranger_configs	1449
list_ranger_hdfs_config	1451
list_ranger_staps	1452
list_ready_files	1453
list_roles	1453
list_roles_granted_to_object_by_Name	1454
list_roles_granted_to_object_by_id	1454
list_rules_with_threshold	1455
list_running_processes	1455
list_scheduler_jobs	1456
list_schedules	1458
list_stap_verification_results	1458
list_staps	1459
list_test_detail_exception	1460
list_test_exception	1460
list_test_exception_by_id	1461
list_user_hierarchy_by_parent_user	1461
list_user_roles	1462
list_users	1463
list_utilization_thresholds	1464
load_all_packages	1464
load_mongodb	1464
load_mongodb_by_datasource	1465
local_disable_big_data_intelligence	1465
local_enable_big_data_interface	1466
make_bundle_with_uploaded_kernel_module	1467
make_primary_cm	1467
migrate_stap_config	1468
modify_autodetect_process	1468
modify_ef_mapping	1469
modify_ef_sql_mode	1470
modify_guard_param	1471
modify_oauth_validity	1478
modify_schedule	1478
modify_va_summary_key	1479
must_gather	1479
non_credential_scan	1480
nsqd	1481
patch_cleanup	1481
patch_install	1481
pause_or_resume_job	1482
pause_or_resume_scenarios	1483
policy_fam_rule_delete	1484

policy_install_	1484
policy_uninstall_	1485
populateMembersForGroup_	1486
populate_from_dependencies_	1486
populate_group_from_query_	1487
proxy_	1488
pull_external_stap_keystore_	1489
push_insights_trust_	1490
push_parameter_to_mu_	1492
quick_search_	1492
reboot_image_universal_connector_	1494
refresh_quick_search_groups_	1494
refresh_stap_info_	1495
register_oauth_client_	1495
register_oauth_internal_client_	1496
register_unit_	1496
reinstall_policy_	1497
reinstall_policy_rule_	1497
remove_all_from_schedule_	1498
remove_all_qr_replace_elements_	1499
remove_all_qr_replace_elements_byId_	1499
remove_classifier_datasource_	1500
remove_classifier_datasource_group_	1500
remove_connection_properties_	1501
remove_custom_property_from_datasource_by_id_	1501
remove_custom_property_from_datasource_by_name_	1502
remove_custom_property_from_datasources_in_group_	1502
remove_datasource_configuration_from_collector_	1503
remove_datasource_from_entitlement_optimization_	1503
remove_datasource_from_group_	1504
remove_dm_from_profile_	1504
remove_domain_from_universal_connector_allowed_domains_	1505
remove_extraction_profile_	1506
remove_members_of_groups_by_desc_	1506
remove_members_of_groups_by_id_	1507
remove_mfa_exempt_users_	1507
remove_objects_native_audit_	1508
remove_populate_group_from_query_	1509
remove_qr_action_	1509
remove_qr_add_where_by_id_	1510
remove_qr_condition_	1510
remove_qr_definition_	1511
remove_qr_replace_element_byId_	1511
remove_ranger_config_	1512
remove_ranger_service_	1513
remove_threshold_from_rule_	1514
replace_active_profile_	1514
reregister_agg_collector_	1515
rerun_datamart_	1515
rerun_distributed_report_	1516
reset_unit_utilization_data_	1516
reset_va_summary_by_id_	1517
reset_va_summary_by_key_	1517
rest_export_definition_	1517
restart_all_managed_units_	1518
restart_cloud_instance_	1518
restart_job_queue_listener_	1519
restart_solr_	1519
restart_stap_	1520
restart_unit_pinger_	1521
restore_units_after_bad_shift_	1521
retrieveUpdatedUsers_	1521
retrieveAPIs_	1522
retrieveApiParameters_	1522
revokeOAuthClient_	1522
revokeOAuthToken_	1523
revoke_api_key_	1523
revoke_ignore_stap_	1523
revoke_role_from_object_by_Name_	1524
revoke_role_from_object_by_id_	1525
riskspotter_set_config_	1525
rule_info_from_policy_	1526
run_custom_table_ldap_import_	1526
run_database_instance_discovery_	1527
run_diagnostics_	1527
run_populate_group_from_query_	1528
run_universal_connector_	1528
sched_cust_table_distribution_	1529
schedule_generate_mongo_filter_job_	1530
schedule_job_	1531

search	1532
secure_settings	1534
session_inference_control	1536
session_inference_setup	1537
setOAuthTokenExpirationTime	1538
set_alerter_settings	1538
set_alerter_smtp_settings	1539
set_alerter_snmp_settings	1539
set_certificate_host_validation	1540
set_debug_level	1541
set_distributed_report_target	1541
set_enterprise_search_options	1542
set_entitlement_datasource_parameter	1543
set_expiration_date_for_restored_day	1543
set_flatLogProcessType	1544
set_health_traffic_job_interval	1545
set_import	1545
set_inapplicable_test_result_status	1546
set_ip_to_alias_overwrites	1546
set_ip_to_alias_selected	1547
set_job_process_concurrency_limit	1547
set_ktap_debug	1548
set_load_balancer_param	1549
set_outliers_detection_demo_mode	1549
set_outliers_detection_parameter	1549
set_outliers_detection_to_factory_settings	1551
set_outliers_user_detection_mode	1552
set_populate_group_from_query_schedule	1552
set_purge_batch_size	1553
set_stap_debug	1553
set_universal_connector_data_timeout	1554
set_universal_connector_log_level	1555
set_user_roles	1556
set_ztap_logging_config	1556
show_alerter_settings	1557
show_alerter_smtp_settings	1558
show_alerter_snmp_settings	1558
show_alerter_status	1559
show_autodetect_process_status	1559
show_backup_cm_ip	1560
show_expiring_certificates	1561
show_maximum_query_duration	1561
show_universal_connector_plugins	1562
solr_repair_analysis	1563
start_istap_monitor	1564
stop_audit_process	1564
stop_autodetect_process	1565
stop_istap_monitor	1565
stop_restart_alerter	1566
stop_solr	1566
stop_universal_connector	1567
store_maximum_query_duration	1568
store_sql_credentials	1569
store_stap_approval	1569
switch_outliers_user_mode	1570
test_datasource_connection	1570
test_hashicorp_connection	1571
test_solr	1571
test_solr_cluster_status	1572
test_solr_connectivity	1572
test_solr_hardware_requirements	1573
unassign_load_balancer_groups	1574
unassign_gr_condition_from_action	1574
uninstall_policy_rule	1575
universal_connector_cleanup	1575
universal_connector_disable_metrics	1576
universal_connector_enable_metrics	1576
universal_connector_keystore_add	1577
universal_connector_keystore_list	1577
universal_connector_keystore_remove	1578
universal_connector_troubleshooting	1578
universal_connector_update_proxy	1579
unregister_unit	1579
unschedule_datamart	1580
update_alias	1580
update_assessment	1581
update_assessment_test	1581
update_aws_secrets_manager_config	1582
update_cas_host_instance	1582
update_cas_template	1583

update_classifier_action	1584
update_classifier_document_rule	1585
update_classifier_log_level	1586
update_classifier_policy	1587
update_classifier_process	1587
update_classifier_rule	1588
update_cloud_datasource	1589
update_computed_attribute	1591
update_constant_attribute	1592
update_custom_table_ldap_import	1592
update_cyberark_config	1593
update_datamart	1594
update_datamart_copy_file_threadpool_params	1594
update_datasource_by_id	1595
update_datasource_by_name	1597
update_datasource_credentials_in_group	1598
update_datasource_custom_property	1599
update_datasource_group	1599
update_engine_config	1600
update_entry_location	1602
update_external_stap_config	1603
update_group_by_desc	1605
update_group_by_id	1606
update_hashicorp_config	1607
update_insights_agent_config	1608
update_insights_registration_config	1608
update_ip_restriction_allowlist	1609
update_istap_config	1610
update_managed_units_ping_time	1611
update_policy	1611
update_policy_analyzer_interval	1612
update_qr_action	1612
update_qr_add_where_by_id	1613
update_qr_condition	1613
update_qr_definition	1614
update_qr_replace_element_byId	1615
update_quarantine_allowed_until	1616
update_quarantine_until	1617
update_ranger_config	1618
update_ranger_hdfs_config	1618
update_ranger_service	1619
update_rule	1620
update_shared_secret	1627
update_stap_config	1627
update_test_detail_exception	1631
update_test_exception	1631
update_threshold_in_rule	1632
update_user	1632
update_user_db	1633
update_utilization_thresholds	1634
upload_custom_data	1634
venafi_import	1635
verify_cyberark_access	1636
verify_stap_inspection_engine_with_sequence	1636
wkc_refresh_external_pwd	1637
Access management APIs	1638
Active threat analytics and risk spotter APIs	1639
Alerter APIs	1639
Archive, export, import, purge, and restore APIs	1639
Assessment APIs	1640
Auto-discovery APIs	1641
Big Data Intelligence APIs	1641
Catalog entry APIs	1641
Central management APIs	1641
Classification APIs	1642
Cloud datasource APIs	1642
Configuration Auditing System APIs	1642
Data mart APIs	1643
Database user APIs	1643
Datasource APIs	1643
Datasource credential management APIs	1644
Entitlement optimization APIs	1645
External feed APIs	1645
File Activity Monitor APIs	1645
Guardium Insights APIs	1645
Guardium Installation Manager (GIM) APIs	1646
Guardium universal connector APIs	1646
Group APIs	1646
Health analyzer APIs	1647
Hadoop monitoring APIs	1647

Investigation Dashboard APIs	1648
Miscellaneous APIs	1648
Native audit APIs	1650
Outliers detection APIs	1650
Policy and rule APIs	1650
Process Control APIs	1651
Query rewrite APIs	1651
Reports and report generation APIs	1652
Schedule and job dependencies APIs	1653
Solr APIs	1653
S-TAP and inspection engine APIs	1653
S-TAP for IBM i APIs	1654
Threat detection analytics APIs	1654

IBM Guardium V12.0

Welcome to the IBM® Guardium® documentation, where you can find information about how to install, maintain, and use IBM Guardium.

Getting started

- [Product overview](#)
- [Product legal notices](#)
- [What's new](#)
- [Release notes](#)
- [Installing](#)
- [Upgrading](#)

Troubleshooting and support

- [Guardium support home](#)
- [Guardium support resources](#)
- [Guardium support videos](#)
- [IBM developerWorks Answers for Guardium](#)

More information

- [IBM data security and protection](#)
- [IBM Security Guardium product information](#)
- [IBM Security Learning Academy](#)
- [IBM developerWorks Guardium community](#)
- [Guardium tech talk videos](#)

© Copyright IBM Corporation 2002, 2023

Product overview

Product and release information for Guardium® Solutions.

- **[IBM Guardium](#)**
IBM® Guardium prevents leaks from databases, data warehouses and Big Data environments such as Hadoop, ensures the integrity of information and automates compliance controls across heterogeneous environments.
- **[What's new in this release](#)**
New features, functions, and enhancements.
- **[Release information](#)**
Learn about the latest features and enhancements, system requirements, installation, upgrade, and support information.
- **[Notices](#)**
This information was developed for products and services offered in the U.S.A.

IBM Guardium

IBM® Guardium® prevents leaks from databases, data warehouses and Big Data environments such as Hadoop, ensures the integrity of information and automates compliance controls across heterogeneous environments.

It protects structured and unstructured data in databases, big data environments and file systems against threats and ensures compliance.

It provides a scalable platform that enables continuous monitoring of structured and unstructured data traffic as well as enforcement of policies for sensitive data access enterprise-wide.

A secure, centralized audit repository combined with an integrated workflow automation platform streamlines compliance validation activities across a wide variety of mandates.

It leverages integration with IT management and other security management solutions to provide comprehensive data protection across the enterprise.

They are intended to enable continuous monitoring of heterogeneous database and document-sharing infrastructures, as well as enforcement of your policies for sensitive data access across the enterprise, utilizing a scalable platform. A centralized audit repository designed to maximize security, combined with an integrated compliance workflow automation application, enables the products to streamline compliance validation activities across a wide variety of mandates.

IBM Guardium is designed to help safeguard critical data. Guardium is a comprehensive data protection platform that enables security teams to automatically analyze what is happening in sensitive-data environments (databases, data warehouses, big data platforms, cloud environments, file systems, and so on) to help minimize risk, protect sensitive data from internal and external threats, and seamlessly adapt to IT changes that may impact data security. Guardium helps ensure the integrity of information in data centers and automate compliance controls.

The IBM Guardium solution is offered in two versions:

- IBM Guardium Database Activity Monitoring (DAM)
- IBM Guardium File Activity Monitoring (FAM) - Use Guardium file activity monitoring to extend monitoring capabilities to file servers.

The IBM Guardium products provide a simple, robust solution for preventing data leaks from databases and files, helping to ensure the integrity of information in the data center and automating compliance controls.

Guardium products can help you:

- Automatically locate databases and discover and classify sensitive information within them;
- Automatically assess database vulnerabilities and configuration flaws;
- Ensure that configurations are locked down after recommended changes are implemented;
- Enable high visibility at a granular level into database transactions that involve sensitive data;
- Track activities of end users who access data indirectly through enterprise applications;
- Monitor and enforce a wide range of policies, including sensitive data access, database change control, and privileged user actions;
- Create a single, secure centralized audit repository for large numbers of heterogeneous systems and databases; and
- Automate the entire compliance auditing process, including creating and distributing reports as well as capturing comments and signatures.

The Guardium solution is designed for ease of use and scalability. It can be configured for a single database or thousands of heterogeneous databases located across the enterprise.

This solution is available as preconfigured appliances shipped by IBM or as software appliances installed on your platform. Optional features can easily be added to your system after installation.

These are the key functional areas of Guardium's database security solution:

- Vulnerability assessment. This includes not just discovering known vulnerabilities in database products, but also providing complete visibility into complex database infrastructures, detecting misconfigurations, and assessing and mitigating these risks.
- Data discovery and classification. Although classification alone does not provide any protection, it serves as a crucial first step toward defining proper security policies for different data depending on its criticality and compliance requirements.
- Data protection. Guardium addresses data encryption at rest and in transit, static and dynamic data masking, and other technologies for protecting data integrity and confidentiality.
- Monitoring and analytics. This includes monitoring of database performance characteristics and complete visibility in all access and administrative actions for each instance. On top of that, advanced real-time analytics, anomaly detection and security information and event management (SIEM) integration can be provided.
- Threat prevention. This refers to methods of protection from cyberattacks such as distributed denial-of-service (DDoS) or SQL injection, mitigation of vulnerabilities that are not patched and other database-specific security measures.
- Access management. This goes beyond basic access controls to database instances. The rating process focused on more sophisticated, dynamic, policy-based access management capable of identifying and removing excessive user privileges, managing shared and service accounts, and detecting and blocking suspicious user activities.
- Audit and compliance. This includes advanced auditing mechanisms beyond native capabilities, centralized auditing and reporting across multiple database environments, enforcing separation of duties, and tools supporting forensic analysis and compliance audits.
- Performance and scalability. Although not a security feature, it is a crucial requirement for all database security solutions to be able to withstand high loads, minimize performance overhead and support deployments in high-availability configurations.

For more information on the Guardium family of products, visit <https://www.ibm.com/security/data-security/guardium>.

What's new in this release

New features, functions, and enhancements.

12.1 and later IBM Guardium V12.1

Audit process

Support is added to customize the audit process emails. For more information, see [Custom email template](#) in [Building audit processes](#).

Certificate management

- The login page now shows the certificate expiration details and provides a link to manage the certificates.
- Manage, update, and distribute all your expiring certificates from a central manager to the central manager and its managed units. For more information, see [Managing expiring certificates](#).
- View all the certificates that expire on the system within a specified threshold. For more information, see [show_expiring_certificates](#).
- Backup and restore process is enhanced for default and custom certificates. For more information, see [Restoring default and custom certificates](#).

Classifier

Support is added for new custom property, maximum length for large-text data types with PostgreSQL and Sybase.

CLI Commands

Support is added for automating the following CLI Commands:

- Restart and Start commands: `restart datastreams, restart GUI, restart insights_Kafka, restart network, restart processmgr, restart rds_monitoring, restart sniffer_buffer_usage, restart stopped_services, restart system, restart ticket-service, restart alerter, restart guardium_insights, restart icap, restart inspection-core, and start insights_Kafka`
- Store commands: `store disk_space_reserved reset, store dump_data_for_forensics, store mysql_utf8mb4, store quartz_thread_num, store remove_informix_driver_property_IFX_USE_STRENC, store system ipmode, store`

- ```
set_informix_driver_property, store system public key reset, and store system
sshd-max-connection.
• Support commands: support store rdsdiag clean, and support
dump_gdm_exception_error.
```

For more information, see [CLI Commands](#).

#### Cross-central manager(CM) health view system

- Manage patches for central managers and its managed units on cross-CM health view systems. For more information, see [Managing patches on a cross-CM health view system](#).
- Register and unregister central managers to the cross-CM health view system from the Patch Management page or by using API. For more information, see [Viewing cross-CM health view deployment health data](#).

#### Database instance discovery

Run database instance discovery from the central manager on all active S-TAP units for managed unit groups or individual managed units by using the GUI. For more information, see [Monitoring managed units](#).

#### Database discovered instances rules

- A new Manage Collectors view was added to the central manager user interface to quickly and easily find the collectors that are participating in the database discovered instances rules processing. From this dialog, the IE\_CREATION parameter for each collector can be viewed and updated.
- The new Discovered instances rules parameters report on the collector shows the timestamp of when the IE\_CREATION parameter was last changed and its current setting.
- Predefined GRDAPI mapping of modify\_guard\_param provides convenience. The IE\_creation parameter can also be viewed or updated from the command line.

For more information, see [database discovered instances rules](#).

#### Deployment health topology

Support is added for monitored processes report that provides combined information about the Investigation dashboard and Threshold alerter. For more information, see [Deployment health topology and table views](#).

#### GIM certificates

Support is added to replace the default SHA2 GIM certificate with SHA1 or SHA256 without interrupting the GIM server to GIM client communication. For more information, see [Replacing default GIM certificate with SHA1 or SHA256 certificate](#).

#### Integration

Ranger HDFS for Hortonworks and Cloudera 7 supports integration with Atlas service.

#### Policies

- Support is added to quarantine the users with multiple failed login attempts for the security incident policies. For more information, see [Quarantine users with multiple failed logins](#).
- Support is added for the following actions in the Session-level policies.
  - Log Full details with replaced values
  - Log Extrusion Counter
  - Log Masked Extrusion Counter
  - Log Only
  - Log Masked Details
  - Audit Only
  - Ignore responses per session
For more information, see [Actions](#).
- Support is added to detect the Canadian Social Insurance Number (SIN) pattern. For more information, see [Special pattern tests](#).

#### Proxy connection

Guardium supports a web proxy to connect to a remote source that requires a proxy server to connect. Use the proxy grdapi to create the proxy connections. For more information, see [proxy](#).

#### Reports

Support is added for Audit Process Task Details, Available VA Tests - CIS, and Available VA Tests - STIG predefined admin reports.

#### S-TAP

- Support is added to schedule S-TAP diagnostics from the S-TAP Diagnostic Scheduler user interface. For more information see, [Scheduling S-TAP diagnostics](#).
- Support is added for S-TAP to deliver encrypted and unencrypted login packets that contain Kerberos username to the Collector. S-TAP matches the session with the Kerberos username by using the Security Support Provider Interface (SSPI) data as the key. The following parameters are added to support this feature: SSPI\_NAME\_LIMIT, SSPI\_NAME\_TTL, SSPI\_SESSION\_TTL, and SSPI\_SESSION\_MEMORY. For more information, see [General parameters](#) and [Protocol 8 General parameters](#).
- The enhanced S-TAP load-balancing feature aims to eliminate data loss during the collector failover process. For more information, see [S-TAP load-balancing models and configuration guidelines](#) for Linux® and Unix, and [S-TAP load balancing models and configuration guidelines](#) for Windows.
- The Internal Load Balancer (ILB) helps avoid data loss caused due to collector overload. For more information, see [S-TAP load-balancing models and configuration guidelines](#) for Linux and UNIX, and [S-TAP load balancing models and configuration guidelines](#) for Windows.
- Support added to increase K-TAP throughput with dynamic ring buffers. For more information, see [Increasing S-TAP and K-TAP throughput with dynamic ring buffers](#).

#### Universal Connectors

Support is added to centrally manage the Guardium Managed Units on which the Universal Connectors are installed. For more information see, [Universal connector configuration](#).

#### Vulnerability Assessment

- Ability to exclude or specify Microsoft SQL to be scanned.

- Addition of Security Technical Implementation Guide (STIG) Oracle Database 19c benchmark.
- Available tests report filters by CIS, CVE, APAR, CAS-based, JDBC-based, and user-defined-JDBC-based.
- Addition of test severity level to the SCAP XML Export.
- CIS Microsoft SQL Server 2022 1.0 benchmark support.
- Entitlement reports for CockroachDB.
- Support is added for DynamoDB.
- Performance enhancement between central manager and managed units.
- Purge of older DPS history for older, major release versions.
- Scanning for Amazon Aurora PostgreSQL.
- Support for namespaces with HashiCorp Vault integration.
- Support of multi-tenancy for Oracle 19c pluggable databases (PDB).
- For a complete list of tests and groups that are added or updated in version 12.1, see [Vulnerability Assessment tests and groups in Guardium 12.x](#). Tests and groups that are added after the release of Guardium version 12.1 are available in the upcoming Quarterly DPS files.

#### Other enhancements

- View and manage the security settings components: sshd, ciphers, services. For more information, see [secure\\_settings](#).
- Archive and export data on target hosts for specified time intervals. For more information, see [aggregation](#).
- Configure a proxy to connect GDP and GI. For more information, see [insights\\_registration](#).
- Use an API key to run REST API authentication, which never expires, to get an access token to make REST API calls to Guardium. For more information, see [create\\_api\\_key](#), [list\\_api\\_key](#), and [revoke\\_api\\_key](#).

## 12.0 and later IBM Guardium V12.0

---

#### Access management

Guardium 12.0 adds "password last changed" and "password expired" dates to the access management page and to the list\_users API output to better support proactive password management.

#### Active threat analytics

You can now optimize resources and reduce false positives by excluding certain sources such as test data and activities that are performed by automated processes.

#### Audit process

- The audit process to-do list adds the ability to quickly change the classification result sets being compared directly from the results-comparison view itself. For more information, see [Comparing discovery and classification results](#).
- You can now modify the receivers list for active audit processes, including deleting and rearranging existing users. Changes are tracked in the "User activity audit trail" report. For more information, see [Audit process receivers](#).

#### Certificate management

- Support is added for automatic retrieval of existing certificates from Venafi using the Guardium CLI.
- The number of SAN (subject alternative name) slots have increased from nine to 99.
- The date format in the warning message under the notification icon for expiring certificates has changed from `d-m-yyyy` to `yyyy-mm-dd`.

#### Classifier

- Support is added for fire with marker option for catalog search rules.
  - Support is added for new custom properties, including maximum length for large-text data types with Microsoft SQL Server and new data-cardinality methods for Oracle.
- For more information, see [MS SQL Server \(DataDirect\)](#), and [Oracle \(Data Direct - Service Name\)](#).

#### Central management

- You can now view patch installation status of managed units from central managers.
- The cross-central-manager health view (cross-CM health view) is a new Guardium unit type that provides aggregated health views for an entire Guardium deployment. These views include health information for all available central managers, aggregators, collectors, and S-TAPs in your environment. For more information, see [Viewing deployment health data from multiple central managers](#).

#### Database discovered instances rules

- Ability to specify existing Guardium groups for filter and exclude rules.
- Ability to delete discovered instances and existing inspection engines that match specified criteria and standard operators.

For more information, see [database discovered instances rules](#).

#### Datasources

Support is added for creating new groups with username and hostname or IP address criteria.

#### Entitlement reporting

Support added for EDB PostgreSQL.

#### External ticketing

Event Management is now integrated with the ServiceNow. For more information, see [Configuring an external ticketing system](#).

#### GIM

Guardium now uses SHA256 GIM client certificates. For more information, see [GIM clients with SHA256 certificates](#).

#### IBM® Knowledge Catalog integration

- You can now use an external credential manager (AWS Secrets Manager, CyberARK, or HashiCorp) to supply credentials to the IBM Knowledge Catalog - Guardium integration.
- The Guardium-IBM Knowledge Catalog integration includes several updates to how PII is captured during an upgrade. For more information, see [Integrating with IBM Knowledge Catalog for federated data protection](#).
- To learn more information about supported datasources for IBM Knowledge Catalog, see [Integrating with IBM Knowledge Catalog for federated data protection](#) and [Adding User-Defined Functions \(UDFs\) for IBM Knowledge Catalog - Guardium integration](#).

#### Investigation dashboard

Support added for monitoring and automatic recovery to identify and recover issues in the investigation dashboard. For more information, see [Monitoring and automatic recovery for the investigation dashboard](#).

#### Network Time Protocol (NTP)

Network Time Protocol (NTP) now uses the chrony time server daemon. The **ntp** CLI commands are deprecated and replaced by **time\_server** commands. For more information, see the [store system time server](#) CLI command.

#### Runtime sensitive-object identifier

The Runtime Sensitive Object Identifier is redesigned. You can now manage runtime sensitive object identification by using the new Runtime Sensitive Object Identifier session level policy and report. For more information, see [Runtime sensitive-object identifier](#).

#### Policies

Session-level policy adds support for SQL criteria, extrusion rules through criteria server data, and the ability to use regex in groups and custom tuples.

#### S-TAP

- Define S-TAP clusters for environments with multiple S-taps that are assigned to clusters of database servers. S-TAP clusters allow Guardium to detect traffic at the cluster level, meaning that if one S-TAP in the cluster is active, all S-TAPs assigned to the cluster are also marked as active. S-TAP clusters also support automatic removal of inactive S-TAP connections for active-passive cluster configurations. For more information, see [Create and manage S-TAP clusters](#).
- Unix S-TAP and External S-TAP support OpenSSL v3.1 and FIPS140-3.
- External S-TAP supports MongoDB Atlas with MongoDB Compass.

#### TLS 1.3 support

Guardium now supports TLS 1.2 and 1.3, and support for earlier TLS versions is deprecated. For more information about moving to TLS 1.3, see [Managing the TLS version](#).

#### Universal connector

- The universal connector now offers a troubleshooting tool. For more information, see [universal connectors](#).
- Universal connector plug-ins are now preinstalled. When newer versions of the plug-ins become available, you can choose to upload them manually or wait for the next Guardium patch release to get them automatically updated.

#### Vulnerability Assessment

- Ability to display both alias and non-alias value in a report.
- Ability to find an existing vulnerability assessment by using the Security Assessment Finder screen.
- Ability to upload MS SQL opensource driver through custom uploads.
- Ability to export vulnerability assessment results through external feed.
- Support added for Oracle MySQL enterprise edition 8.0 CIS benchmark version 1.2.0, MongoDB 4.0 and MongoDB 5.0 CIS benchmark version 1.0.0, latest CIS benchmark for Db2, CIS benchmark for PostgreSQL version 15.
- Support added for Oracle MySQL enterprise edition 8.0 STIG benchmark, ver 1 rel 1, Oracle 19c benchmark.
- SSL encryption support is added for Oracle 11.x, 12.x, and 19.
- Support added for Apache Cassandra, Percona MySQL datasources.
- Support added for Apache Cassandra, PostgreSQL, and PostgreSQL EDB entitlement reports.

For a complete list of tests and groups that are added or updated in version 12.0, see <https://www.ibm.com/support/pages/node/7031317>. Tests and groups that are added after the release of Guardium version 12.0 are available in upcoming quarterly DPS reports.

#### Other enhancements

- RHEL is upgraded from RHEL 7 to RHEL 9
- The output of all CLI commands (including Guardium API commands) that modify a component of the user's system now includes the timestamp after the command finishes running.
- Ability to mark updates as "read" from the notification icon in the UI.

---

## Release information

Learn about the latest features and enhancements, system requirements, installation, upgrade, and support information.

---

### Release announcement

See the IBM Guardium release announcement for the following information:

- Detailed product description, including a description of new functionality
- Product-positioning statement
- Packaging and ordering information
- International compatibility information

---

### Release notes

For new features, enhancements, and other detailed release-related information, see the IBM Guardium detailed release notes:

12.1 [Guardium 12.1 release notes](#).

12.0 [Guardium 12.0 release notes](#).

---

## System requirements

For Guardium versions 11.0 and later, most supported platforms information is available through the [Guardium support matrix](#).

For all other supported platforms and system requirements information, including vulnerability assessment, platforms supported by external S-TAP, information about IBM i, and hardware or VM requirements, see:

- 12.1 [System Requirements for Guardium® 12.1](#)  
12.0 [System Requirements for Guardium 12.0](#)

For technical support and other resources, search the [IBM Support](#) website.

## Hardware requirements

---

For detailed hardware specifications and sizing recommendations, see:

- 12.1 [Appliance Technical Requirements for Guardium 12.1](#)  
12.0 [Appliance Technical Requirements for Guardium 12.0](#)

## Installing and upgrading Guardium

---

For installation instructions, see [Installing your Guardium system](#).

For information about upgrading to the latest version of Guardium, see [Upgrading your Guardium system](#).

If you are using an older version of Guardium software, plan ahead to allow time for upgrades. You can find information about end-of-support dates for IBM products at the [IBM Software Support Lifecycle](#) website.

For up-to-date help, access the documentation landing page for IBM Guardium: <https://www.ibm.com/docs/guardium>

---

## Notices

This information was developed for products and services offered in the U.S.A.

This material may be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM® may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:** INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
US.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of

non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

#### COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Depending on how you are viewing this information, some images and illustrations may not appear.

## Trademarks

---

IBM, the IBM logo, and ibm.com® are trademarks or registered marks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at: <http://www.ibm.com/legal/copytrade.shtml>.

Adobe, the Adobe logo, Postscript, and the Postscript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux® is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

## Terms and conditions for product documentation

---

Permissions for the use of these publications are granted subject to the following terms and conditions:

**Applicability:** These terms and conditions are in addition to any terms of use for the IBM website.

**Personal use:** You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

**Commercial use:** You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

**Rights:** Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

## Privacy policy considerations

---

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at <http://www.ibm.com/privacy>.

## FIPS 140-2

---

When in FIPS 140-2 mode, IBM Security Guardium uses the FIPS 140-2 approved cryptographic provider(s); IBMJCEFIPS (certificate 376) and/or IBMJSSEFIPS (certificate 409) and/or IBM Crypto for C (ICC (certificate 384) for cryptography. You can search for the certificates at the NIST web site at <https://csrc.nist.gov/>.

# Getting started

- [Components and topology](#)  
Learn about Guardium appliances, agents, and other components.
- [Getting started with the user interface](#)  
Learn the basics of the Guardium user interface, including logging in for the first time, banner and navigation menus, and the user interface and data search.
- [Customizing the user interface](#)  
Guardium® supports customizing the navigation menu for specific users and roles.
- [Identifying and investigating risks: getting started](#)  
Guardium's Active Threat Analytics, Risk Spotter, and Investigation Dashboard give you both a bird's eye view of potential risks in your system, risk trends over time, and tools to investigate the potential risks. Incorporate these tools into your daily Guardium routine to increase your abilities to identify and manage risks.
- [Smart assistant for monitoring and compliance](#)  
Learn how to deploy monitoring agents to your database servers and configure database monitoring for compliance with security standards and regulations.
- [System view](#)  
The System View is the default initial view for many users. It enables you to see key elements of system status.
- [Data activity monitoring](#)  
Information about key security concepts used in Guardium data activity monitoring.
- [File activity monitoring on Windows and Unix-Linux file servers](#)  
File Activity Monitoring discovers the sensitive data on your servers; classifies content using pre-defined or user defined definitions; configures rules and policies about data access, and actions to be taken when rules are met.
- [File activity monitoring for NAS and SharePoint](#)  
Guardium monitors file activity, and perform discovery and classification on NAS devices and SharePoint servers in a Windows environment.
- [Key concepts and tools](#)  
Information about key concepts pertaining to Guardium administration.

## Related information

- [IBM Security Guardium product information](#)

## Components and topology

Learn about Guardium appliances, agents, and other components.

### Guardium components

- Guardium systems:
  - Collectors: The collector performs real-time capture and analysis of the database activity, and logs it for further analysis and use in alerting.
  - Aggregators: Guardium aggregators collect and merge information from multiple Guardium collectors, and optionally from other aggregators. They produce holistic views of an entire environment. Collection and aggregation processes allow Guardium to easily generate enterprise-level reports. In a large enterprise environment, for example, several Guardium systems can be used for monitoring different geographic locations or business units. You can export data from multiple collectors to a single aggregator, and view database usage across all geographic areas or business units. Reports, assessments, and audit processes run from this aggregator would then reflect data collected from across the environment.
  - Central Managers: The central manager (CM) is a specialized functionality that is enabled on an aggregator. In this configuration, one Guardium system is designated as a central manager that controls and monitors an entire Guardium environment, from a single console. In this configuration, collectors and aggregators are referred to as managed units. While some applications (Audit Processes, Queries, Portlets, etc.) can be run from either a managed unit or from the central manager, application's definitions are stored on the central manager. See [Aggregation and central management](#). Central management supports hierarchical aggregation where multiple aggregators merge their data repositories to a central aggregator. This is useful for multi-level views. For example, with different Guardium aggregators assigned to different geographic locations, a central management aggregator can merge the contents of all aggregators into a single global view spanning all geographies. See [Data aggregation](#).
- To set up your central manager and managed units for Vulnerability Assessment (VA), see [Set up your environment for Vulnerability Assessment](#).
- Agents (required and most common):
  - Software TAP agent (S-TAP): [Windows: S-TAP user's guide](#) and [Linux and UNIX systems: S-TAP user's guide](#).
  - Guardium Installation Manager agent (GIM): The GIM server is installed as part of the Guardium system. It communicates with the GIM client, that is installed on servers that host databases or file systems that you want to monitor. It facilitates agent installation and updating and configuration modification of agents. See [Guardium Installation Manager](#).
  - Change Audit System agent (CAS): The CAS agent is installed on the database server. It captures change audit information of configuration files and more on the database server. See [Configuration Auditing System \(CAS\)](#).
  - Instance Discovery agent: The instance discovery agent is installed on the database server and sends database, listener, and port information to Guardium.
- Datasource: A Guardium datasource identifies a specific database instance. Access to datasources may be restricted based on the roles assigned to the datasource and to the applications that use it. For example, the Value Change Auditing application requires a high level of administrative access that would not be appropriate for other less privileged applications.
- Inspection engine: neither a component nor an agent, an inspection engine is a required configuration that specifies the database platform and the instances that the S-TAP monitors on the S-TAP host (database server). One S-TAP often has many inspection engines.

### Guardium topology

- Basic stand-alone architecture: The most basic architecture is for monitoring several databases in one data center: one stand-alone collector appliance and several Guardium S-TAP agents that are installed on the monitored database servers. The S-TAP agents capture and send the relevant database activities to the one Guardium collector for analysis, parsing, and logging.
- Mid-size architecture: The mid-size architecture monitors numerous databases across data centers. It consists of multiple collector appliances and numerous S-TAP agents that are installed on the monitored database servers in each data center. The S-TAP agents capture and send the relevant database activities to the Guardium collectors for analysis, parsing, and logging. The collectors aggregate activities that are monitored to an aggregator appliance for central reporting. In this example, the aggregator appliance is also serving as the central management appliance for the solution that enables federated management capabilities, such as Access Management, patching, and metadata repository.

- Enterprise architecture: The enterprise architecture monitors numerous databases across multiple data centers and continents. This architecture example consists of many collector appliances and numerous S-TAP agents that are installed on mainframe and distributed database servers across data centers. The S-TAP agents capture and send the relevant database activities to the Guardium collectors for analysis, parsing, and logging. The collectors aggregate activities that are monitored to the respective aggregator appliance for central reporting. A dedicated Central Manager appliance provides federated management capabilities, such as Access Management, patching, and metadata repository.

## Getting started with the user interface

Learn the basics of the Guardium user interface, including logging in for the first time, banner and navigation menus, and the user interface and data search.

### Navigation

When you first log in to the Guardium user interface, there are two main menus - the banner and the navigation menu.

You can expand and collapse the navigation menu by clicking the chevron icon  , or you can hide the navigation menu completely by clicking the show / hide icon 

The initial layout of your screen is determined by the license that is applied, the access allowed based on roles, the machine type, and a visibility factor. Examples of roles are user, admin, access manager, and CLI. Roles are assigned to users and applications to grant users specific access privileges.

### Banner Menu

The banner contains the following items:

Table 1. Banner menu

| Item                         |                                                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System time clock            |                                                                                   | The universal time on your Guardium system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| To-Do List                   |  | Contains the Audit Process To-Do List, which can be filtered by user, and the Processes With No Pending Results.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Help                         |                                                                                   | Open the product help by clicking Help  .Guardium Help.<br>Get information about your Guardium system, such as the version number, by clicking Help  .About Guardium.<br><br>For help content specific to a screen or feature you're working with, click  that is embedded in each page.<br>Note: However you access the Help, when you open same Information Center, where you can search and access all help content. |
| User interface / data / file |                                                                                   | Select Data or File and click  to open the Investigation Dashboard.<br>Select User Interface to search the UI. For example, if you want to find the Policy Builder, type policy builder in the User Interface Search. Click any of the results to go to that part of the user interface.                                                                                                                                                                                                                                                                                                    |
| Account type                 |                                                                                   | Indicates the account type that you logged in with. Edit your account details, such as your password or name, customize UI layout, and sign out of Guardium securely.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Machine type                 |                                                                                   | Indicates what type of Guardium system you are on, such as stand-alone, managed unit, central manager, or aggregator.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

The banner menu also contains important startup messages such as Low RAM memory, Quick Search memory, and CPU 4-cores minimum requirement, Certificate expiration, Central Management failure, SSLv3 enabled or disabled, and No License.

Note: Guardium recommends that SSLv3 be disabled. However, in dealing with older Guardium versions that do not have the latest release installed, if SSLv3 is disabled, the Central Management functionality is impaired between the Central Manager and the managed units.

### Navigation Menu

Each icon in the navigation menu represents one phase of the Guardium security lifecycle, click any icon to expand it and see the components within the phase. The lifecycle-centric navigation menu is one way to navigate the user interface and is consistent across roles. Menu items can be customized and do or don't appear based on your role.

| Phase       |                                                                                     | Description                                                                                                                                                                                      |
|-------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Setup       |  | Configure your network settings, check the status of your services, and setup datasource definitions, groups, aliases, and alerts.                                                               |
| Manage      |  | Manage your environment's overall health, S-TAPs, data, modules, maintenance, and reports.                                                                                                       |
| Discover    |  | Automatically discover new databases that are introduced to your environment, and find and classify sensitive data.                                                                              |
| Harden      |  | Assess your environment's current weaknesses with Vulnerability Assessment and monitor changes that are made to your environment with Configuration Auditing System (CAS).                       |
| Investigate |  | Monitor database activities and investigate suspicious activity in any part of your environment.                                                                                                 |
| Protect     |  | Protect your environment with data security policies that block suspicious activity and prevent unauthorized access to data. For more information about policies, see <a href="#">Policies</a> . |
| Comply      |  | Reach compliance initiatives with audit processes and granular reporting.                                                                                                                        |
| Reports     |  | Create your own report or use one of many predefined reports to report on any part of your environment. For more information about reports, see <a href="#">Reports</a> .                        |

| Phase         |  | Description                                                                                                                                                                                  |
|---------------|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| My Dashboards |  | Create your own dashboards to easily review reports that are of primary interest to you. For more information about dashboards, see <a href="#">Creating dashboards and adding reports</a> . |

## Commonly Found Icons

Many of the finder and builder applications in Guardium share this set of icons.

| Icon   | Description                                                                                                        |
|--------|--------------------------------------------------------------------------------------------------------------------|
| New    | Create an item, such as a group or datasource definition.                                                          |
| Modify | Modify an item.<br>Note: When you modify items, the best practice is to clone the item, and then modify the clone. |
| Clone  | Clone an item to create a copy of the item.                                                                        |
| Delete | Delete an item.                                                                                                    |

## Customizing the user interface

Guardium® supports customizing the navigation menu for specific users and roles.

The Customize Navigation Menu and Customize User/Role tools allow you to conveniently change the content and organization of the navigation menu. You can access these tools in several locations:

- All users can customize their own navigation menu by opening the User menu in the Guardium banner and selecting Customize.
- Administrative users can customize the navigation menu for other users and roles by opening the User menu and selecting Customize User/Role or by navigating to Setup > Tools and Views > Customize User/Role.
- Users logged in as `accessmgr` can customize the navigation menu for other users and roles by navigating to Access > Access Management, selecting Role Browser, and clicking the Customize Navigation Menu link.

The tool provides a consistent customization experience for all users.

The Navigation Menu list reflects the organization and contents of the Guardium navigation system. Select tools and reports from the Available Tools and Reports list and use the icon to add items to the Navigation Menu list. Remove items from the Navigation Menu list by clicking the icon next to an item. Use drag and drop or the icon controls to rearrange items within Navigation Menu list.

It is possible to define a new Guardium home page (that is, the first page seen after logging into the system) by selecting an item from the Navigation Menu list and clicking the icon.

After clicking the OK button, the Guardium navigation menu is updated to reflect any changes you made in the Navigation Menu list.

The following limitations apply when using these tools:

- You cannot delete the My Dashboards group, but you can delete individual dashboards within the group.
- New groups that are empty will not be saved.
- Empty groups shown in the Navigation Menu list will not appear in the Guardium navigation menu.

## Related concepts

- [Managing roles and permissions](#)

## Identifying and investigating risks: getting started

Guardium®'s Active Threat Analytics, Risk Spotter, and Investigation Dashboard give you both a bird's eye view of potential risks in your system, risk trends over time, and tools to investigate the potential risks. Incorporate these tools into your daily Guardium routine to increase your abilities to identify and manage risks.

### [Active Threat Analytics](#)

Active Threat Analytics shows potential security breach cases, based on the outlier mining process and identified attack symptoms. Use its dashboard to view and investigate cases, and take actions on individual cases.

### [Risk Spotter](#)

Risk Spotter is a First of its Kind technology, changing the security paradigm to an Artificial Intelligence Data Protection Policy. It uses a smart algorithm to search within and outside your policy radar (your installed policies), and it uses a holistic algorithm to dynamically assess risk factors. Its dynamic risk assessment considers many risk factors, including: outliers, vulnerability, volume of activities, access to sensitive data, type of commands (privileges). Risk Spotter presents the risky users and risk trends across your entire system, in easy to read graphs. The Risk Spotter page contains all the configuration and results, and actions you can take.

### [Investigation Dashboard](#)

The Investigation Dashboard provides powerful tools for identifying and assessing problems that might exist in your Guardium environment. It uses either local or system-wide unfiltered data, and provides numerous filter options to query data across an entire Guardium environment, potentially from any Guardium collector within that environment.

## Smart assistant for monitoring and compliance

Learn how to deploy monitoring agents to your database servers and configure database monitoring for compliance with security standards and regulations.

## About this task

---

Smart assistant for monitoring and compliance is comprised of the following two tools:

### Deploy monitoring agents

Use the Deploy Monitoring Agents tool to automatically activate GIM clients, install S-TAPs, and begin monitoring database traffic.

The Deploy Monitoring Agents tool simplifies the process of establishing a Guardium deployment. Building on existing Guardium Installation Manager (GIM) infrastructure, the Deploy Monitoring Agents tool helps you quickly find database servers, install monitoring agents (S-TAPs), and configure inspection engines for your databases. In addition, the tool provides a centralized view for tracking and reviewing deployment status.

### Compliance monitoring

After deploying monitoring agents (S-TAPs), use the Compliance Monitoring tool to establish monitoring for specific security standards and regulations.

Guardium provides several compliance monitoring templates--groups, security policies, and reports corresponding to specific standards and regulations--including the following:

- Basel Committee on Banking Supervision (BASEL II)
- General Data Protection Regulation (GDPR)
- General Data Protection Regulation for Db2 for z/OS (GDPR for Db2 for z/OS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Security Standard (PCI)
- Personally Identifiable Information (PII)
- Sarbanes-Oxley Compliance (SOX)

These compliance monitoring templates are especially useful for organizations that must comply with one of the associated standards or regulations in a short period of time. After installing security policies, the compliance monitoring tool guides administrators or compliance officers through the initial setup and population of groups with organization-specific information such as client IP addresses and specific privileged user IDs. In addition, the compliance monitoring tool periodically checks your Guardium environment for new databases that can be monitored using the compliance monitoring templates.

## Procedure

---

1. Review the following information to begin familiarizing yourself with the tools.
  - [Smart assistant for deploying monitoring agents](#)
  - [Smart assistant for compliance monitoring](#)
2. Deploy monitoring agents for your database servers.
  - a. Verify that you have met the prerequisites for using the Deploy Monitoring Agents tool: [Prerequisites for deploying monitoring agents](#).
  - b. Deploy monitoring agents to your database servers: [Deploy monitoring agents](#).
3. Configure compliance monitoring for your database servers.

## Results

---

After successfully deploying monitoring agents and configuring compliance monitoring for your database servers, Guardium begins monitoring your database traffic.

For more information about interpreting what you see on the compliance monitoring dashboard, see [Compliance summary](#).

## System view

---

The System View is the default initial view for many users. It enables you to see key elements of system status.

Three tabs under the System View display different types of status information:

- The S-TAP Status Monitor displays summary data about S-TAPs that are deployed in your environment. Icons represent the high-level status, and you can drill down to view information about inspection engines.
- The Unit Utilization tab displays information about the usage of each Guardium® system.
- The System Monitor tab displays up-to-date details about incoming data, CPU usage, and other information.

## Data activity monitoring

---

Information about key security concepts used in Guardium data activity monitoring.

- [Policies and rules](#)

A security policy contains an ordered set of rules to be applied to the observed traffic between database clients and servers. Each rule can apply to a request from a client, or to a response from a server. Multiple policies can be defined and multiple policies can be installed on a Guardium system at the same time.

- [Workflows](#)

Workflows consolidate several database activity monitoring tasks, including asset discovery, vulnerability assessment and hardening, database activity monitoring and audit reporting, report distribution, sign-off by key stakeholders, and escalations.

- [Auditing](#)

Guardium provides value change auditing features for tracking changes to values in database tables.

- [Classification](#)

Guardium supports the discovery and classification of sensitive data to allow the creation and enforcement of effective access policies.

## Policies and rules

A security policy contains an ordered set of rules to be applied to the observed traffic between database clients and servers. Each rule can apply to a request from a client, or to a response from a server. Multiple policies can be defined and multiple policies can be installed on a Guardium system at the same time.

Each rule in a policy defines a conditional action. The condition can be a simple test, for example a check for any access from a client IP address not found in an Authorized Client IPs group, or the condition can be a complex test that evaluates multiple message and session attributes such as database user, source program, command type, time of day, etc. Rules can also be sensitive to the number of times a condition is met within a specified timeframe.

The action triggered by the rule can be a notification action (e-mail to one or more recipients, for example), a blocking action (the client session might be disconnected), or the event might simply be logged as a policy violation. Custom actions can be developed to perform any tasks necessary for conditions that may be unique to a given environment or application.

## Workflows

Workflows consolidate several database activity monitoring tasks, including asset discovery, vulnerability assessment and hardening, database activity monitoring and audit reporting, report distribution, sign-off by key stakeholders, and escalations.

Workflows are intended to transform database security management from a time-consuming manual activity performed periodically to a continuously automated process that supports company privacy and governance requirements, such as PCI-DSS, SOX, Data Privacy and HIPAA. In addition, workflows support the exporting of audit results to external repositories for additional forensic analysis via Syslog, CSV/CEF files, and external feeds.

For example, a compliance workflow automation process might address the following questions: what type of report, assessment, audit trail, or classification is needed, who should receive this information and how sign-offs are handled, and what is the schedule for delivery?

## Auditing

Guardium provides value change auditing features for tracking changes to values in database tables.

For each table in which changes are to be tracked, you can select which SQL value-change commands to monitor (insert, update, delete). Before and after values are captured each time a value-change command is executed against a monitored table. This change activity is uploaded to Guardium on a scheduled basis, after which all of Guardium's reporting and alerting functions can be used.

You can view value-change data from the default Values Changed report, or you can create custom reports using the Value Change Tracking domain.

## Classification

Guardium supports the discovery and classification of sensitive data to allow the creation and enforcement of effective access policies.

A classification policy is a set of rules designed to discover and tag sensitive data elements. Actions can be defined for each rule in a classification policy, for example to generate an email alert or to add a member to a Guardium group, and classification policies can be scheduled to run against specified datasources or as tasks in a workflow.

Discovery and classification routines become important as the size of an organization grows and sensitive information like credit card numbers or personal financial data become present in multiple locations, often without the knowledge of the current administrators responsible for that data. This frequently happens in the context of mergers and acquisitions, or when legacy systems have outlasted their original owners. Guardium classification discovers and tags this sensitive data so appropriate access policies can be applied.

## File activity monitoring on Windows and Unix-Linux file servers

File Activity Monitoring discovers the sensitive data on your servers; classifies content using pre-defined or user defined definitions; configures rules and policies about data access, and actions to be taken when rules are met.

File activity monitoring consists of the following capabilities:

- Discovery includes collecting metadata and entitlements for files and folders.
- Classification uses *decision plans* to identify potentially sensitive data in the files, such as credit card information or personally identifiable information.
- Monitoring and collection of audit information and policy rules, and real time alerts or blocking of suspicious users or connections.
- [\*\*File activity monitoring functionality\*\*](#)  
FAM functionality on Windows and UNIX file servers is similar to data monitoring. Understand the similarities and differences.
- [\*\*High level workflow for file activity monitoring\*\*](#)  
Use this general workflow to plan and execute file activity monitoring on file servers in the Linux, Unix and Windows environments.

## File activity monitoring functionality

FAM functionality on Windows and UNIX file servers is similar to data monitoring. Understand the similarities and differences.

[FAM Support](#) lists the supported platforms for FAM discovery, classification, and monitoring.

Figure 1. FAM functionality in UNIX file servers

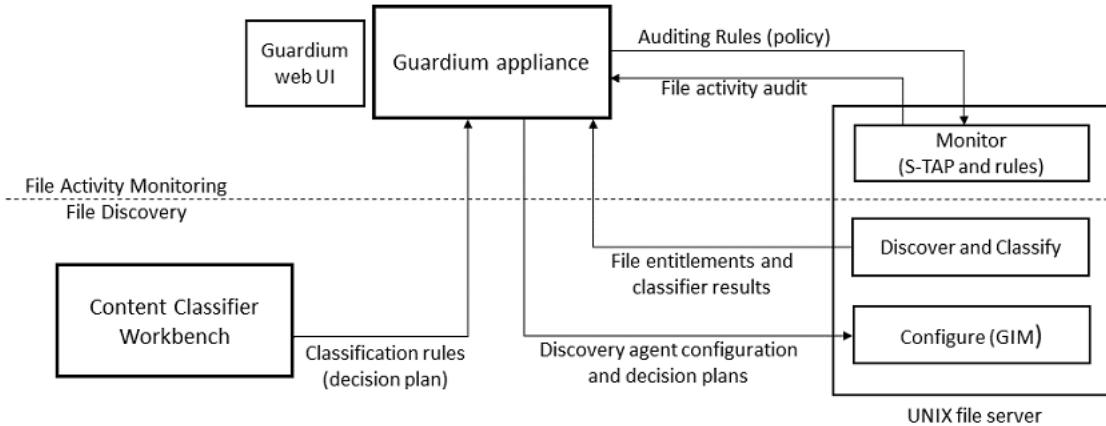
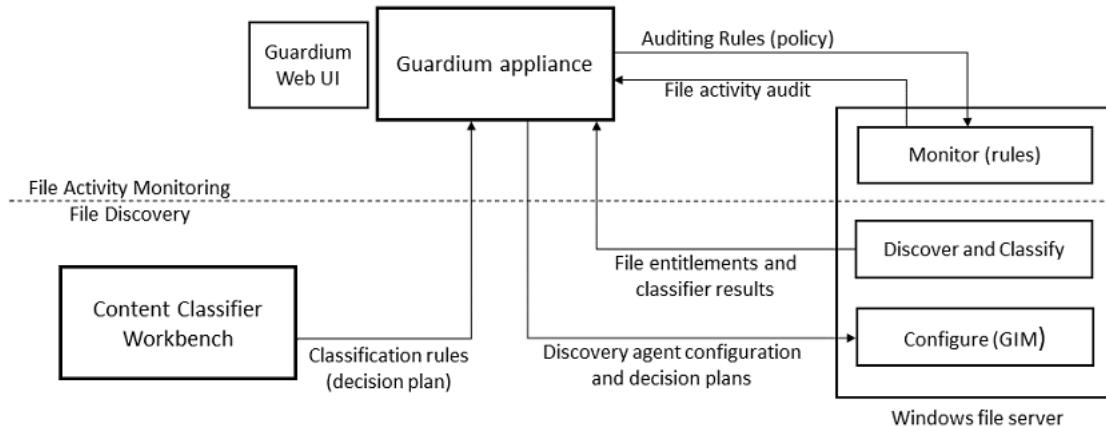


Figure 2. FAM functionality in Windows file servers



#### Discovery and classification

FAM discovery and classification (Windows file system, AIX file system, Red Hat, and Ubuntu) give entitlement and content classification details of given file server folders. Based on its results, you can create smart policies, define groups, and audit their files, focusing on the important assets (by using FAM monitoring).

The basic discovery scan identifies the list of folders and files, their owner, access permissions, size, and the date and time of the last update. It also identifies user permissions and group permissions. Discovery supports all file types. Classification is defined by decision plans. Each decision plan contains rules for recognizing a certain type of data. (Decision plans for File Activity Monitoring are analogous to classification policies for Data Activity Monitoring.) FAM classification for Linux® and Windows is based on [IBM Content Classification](#). Classification supports many types of files, including: Plain text, HTML, Office, PDF, PST (Microsoft Outlook folder; Microsoft Outlook must be installed), and NSF (Lotus Notes® database) format. Lotus Notes is not required but NSF is supported by running a script that is installed with IBM® Content Classification. For complete lists of supported text types, see [What data types are supported](#) and Oracle Text Supported Document Formats in Oracle documentation. Default decision plans exist for HIPAA, PCI, SOX, and Source Code. You can change the classification entities from the resulting reports or investigation dashboard, by using the default decision plans. In addition, you can create new plans, or modify existing plans, by using the Content Classifier workbench, a Windows application you upload to your collector appliance. See the requirements for IBM Content Classification Version 8.8, in the <http://www-01.ibm.com/support/docview.wss?uid=swg27020838> IBM technote. Plans are activated and configured through the Guardium® Installation Manager (GIM).

Discovery and classification are handled by a discovery agent, called the file crawler. The file crawler sends the file metadata, and data from its discovery and classification processes, to the Guardium system. The scan schedule is configurable. Subsequent (incremental) scans, after initial discovery and classification, identify incremental changes of new and changed files only. Install and configure the file crawler with the Guardium Installation Manager (GIM) just as you would any other bundle.

#### Monitor, Audit, and Block

FAM monitors, alerts, and blocks file access according to the Guardium policy rules. The rules specify which file servers and files to monitor and what actions to take if policy rules are violated, for example, log the violation, alert, or block access. Monitored Operations are Read, Write, Execute, Delete, Change Owner, Permissions, Properties. Any activity that matches the security policy rules criteria is sent to the Guardium collector where it is stored in the Guardium repository. (FAM is different from database activity monitoring, where the S-TAP sends all data activity to Guardium for monitoring.) All events that are recorded in the Guardium repository are audited events.

In UNIX servers, file activity monitoring is implemented by the S-TAP, running on the file server. For NFS volumes, it is important that an S-TAP installed and configured on all servers that access those volumes. One S-TAP agent can manage both file server and database activity monitoring. If you have licenses for both capabilities, you can use the same S-TAP agent for both file and database activity monitoring. Install and configure S-TAP with the Guardium Installation Manager (GIM) just as you would any other bundle.

In Windows servers, file activity monitoring is implemented by the FamMonitor bundle. It is installed independently from S-TAP.

UID chain for FAM: FAM identifies the process and the user that performed the access (and not external programs). For instance if Process 1 (`user janedoe`) creates Process 2 (`user johndoe`), then for file events that are related to process 2, FAM reports the UID chain of `{janedoe, johndoe}`. For example,

```
(1,root,systemd)>(10077,root,sshd)>(50136,root,sshd)>(50169,donald,sshd)>(50170,donald,bash)->(50217,donald,ls)
```

UID chain is always enabled in Windows databases. For Linux-Unix, enable the UID chain with the `hunter_trace` parameter. For more information, see [Linux-Unix: General Parameters](#).

Monitoring activities are presented in the following predefined reports: **Users privileges**, **File privileges**, **Count of activity per user**, **Count of activity per client**, **Files open to “public”**, **Dormant users**, **Dormant Files**, and others. In addition, monitoring activities are also shown in the **FAM – Access report** (log of all monitored activity), and in the Investigation Dashboard.

Access to files can also be blocked, even if the operating system permissions allow access. The rules are preinstalled into the S-TAP, which then loads them into the file system filter driver. The driver blocks access to the file so that the data in the file is never delivered to the user.

Important: Windows Administrator and Linux ROOT user activities are not monitored or blocked by File Activity Monitoring.

## High level workflow for file activity monitoring

Use this general workflow to plan and execute file activity monitoring on file servers in the Linux, Unix and Windows environments.

Prerequisites:

- FAM license keys must be installed.
- For UNIX file servers: S-TAP for FAM is installed.
- For Windows file servers: FamMonitor bundle is accessible
- CentOS v7.9 requires that the following libraries are installed: **32-bit libstdc+5 and libstdc+6**
- FAM discovery agent (also known as the FAM bundle or FAM agent) must be accessible. Required for file discovery and classification. Download from [Fix Central](#) or obtain from your Guardium representative.
- Disk space requirements for FAM bundle: 2GB. AIX platforms require an additional 2GB during installation.
- To install the FAM discovery agent successfully on AIX, it is recommended to set the process data size to unlimited. Access the file `/etc/security/limits` and change this line to **default: data = -1**.
- Supported servers and platforms are listed in <https://supportcontent.ibm.com/support/pages/node/6245402>.
- For complete lists of supported data types, see [What data types are supported](#) and Oracle Text Supported Document Formats in Oracle documentation.

**Windows servers only:** From V11.0, the FAM monitor package is a standalone package, and is installed independently. (It is not installed with S-TAP, as it was in previous releases.) When upgrading to v11.0, whether or not you use the GDPR accelerator:

- If you're using FAM and S-TAP: Upgrade the STAP to 11.0. This uninstalls the previous FAM (FsMonitor driver and StapAT service). Then install the 11.0 FAM crawler and FamMonitor.
- If you're using FAM only: Uninstall the S-TAP. This uninstalls the previous FAM (FsMonitor driver and StapAT service). Then install the 11.0 FAM crawler and FamMonitor.

## FAM GDPR Accelerator

Use the FAM GDPR Accelerator to guide you through the entire process of enabling and configuring FAM, including for GDPR compliance. The Accelerator supports Windows, Linux, and UNIX platforms.

1. Access the Module upload page: Accelerators > GDPR > Assess > Prepare > Upload FAM Module for GDPR, and upload the FAM module.
2. Follow the instructions in the GDPR Accelerator GUI page to complete the FAM GDPR configuration. See the overview in Accelerators > GDPR > GDPR Compliance.
3. See the rules that can be used to create decision plans for FAM GDPR in [Rules for GDPR File Activity](#).

## FAM without GDPR Accelerator

If you are not using the FAM GDPR Accelerator, use this workflow for file activity monitoring:

1. Install the FAM crawler for discovery and classification.
  - a. For UNIX file servers. This also installs the monitoring capabilities: [Installing and activating the FAM discovery agent \(crawler\) on UNIX servers](#).
  - b. For Windows file servers: [Installing and activating FAM discovery agent \(crawler\) on Windows servers](#).
  - c. Configure [File discovery and classification GIM parameters](#).
2. Windows servers only: Install the FamMonitor installation package, see [Installing and activating the FamMonitor on Windows servers](#).
3. Monitor and investigate results:
  - Review File activity in reports, including the following predefined reports: File Activities, File Entitlement, Files Count of Activity Per Client, Files Count of Activity Per Server, Files Count of Activity Per User, Files Privileges.
  - For ongoing investigation and analysis, use Investigation Dashboards, which include text search and outliers capability as well as enhanced visualizations. See:
    - [Investigation Dashboard for files](#)
    - [Interpreting file activity outliers in the investigation dashboard](#)
4. Protect: create and apply policies for ongoing monitoring and protection for file servers. See [File Activity policies for UNIX and Windows file servers](#).  
Note: FAM rules might not be applied to certain operations on file descriptors, such as changing the owner or permissions for a file, on these platforms:
  - AIX
  - 12.1 and later Solaris

## File activity monitoring for NAS and SharePoint

Guardium monitors file activity, and perform discovery and classification on NAS devices and SharePoint servers in a Windows environment.

- For monitoring of activity across files and directories residing on NAS devices and SharePoint in the Windows environment, see [File Activity Monitor for NAS and SharePoint](#).

- For discovery, entitlement and classification of files and directories residing on NAS devices and SharePoint in the Windows environment, see [Discovery and Classification for NAS and SharePoint](#).

## Key concepts and tools

Information about key concepts pertaining to Guardium administration.

- [Queries and reports](#)

Guardium queries describe a set of information obtained from the collected data. Each query has a corresponding report with the same name.

- [Access control](#)

Guardium provides access maps as a way to conveniently show data access between database clients and database servers.

- [User roles](#)

A role defines a group of Guardium users who share the same access privileges.

- [Groups](#)

Guardium supports the grouping of elements to simplify creating and managing policies and to clarify the presentation of reports.

- [Data archive and purge](#)

Data Archive backs up data that has been captured by a Guardium system. When configuring Data Archive, data purge criteria may also be specified.

- [Guardium Installation Manager](#)

The Guardium Installation Manager (GIM) is used to install and maintain Guardium components on managed systems.

## Queries and reports

Guardium queries describe a set of information obtained from the collected data. Each query has a corresponding report with the same name.

Guardium queries describe a set of information obtained from the collected data. Queries are based on three elements: entities, fields, and conditions. Entities define the scope of a query, fields list the columns of data to be returned by the query, and conditions define tests to match against the data (greater than, less than, contains, etc.)

The default report is a tabular report, with each attribute displayed in a separate column. All runtime parameters and presentation components of a tabular report can be customized.

## Access control

Guardium provides access maps as a way to conveniently show data access between database clients and database servers.

Data access by applications and tools can be categorized according to many dimensions, including what data is being accessed, how it is being accessed, or how many SQL calls are being made. In an enterprise environment, it is very important to get a good handle on database access. This requirement can stem from the need to understand and secure access to the database due to compliance initiatives and even due to the need to tune and optimize your database environment. Because there can be many databases and a very large number of database clients in enterprise environments, getting a handle on the data access paths can be difficult.

The deployment health topology and table views show the data flow relationships between systems in your environment. These views make it easy to identify problematic systems and investigate the underlying issues. Access the topology view by navigating to [Manage > System View > Deployment Health Topology](#). Access the table view by navigating to [Manage > System View > Deployment Health Table](#).

## User roles

A role defines a group of Guardium users who share the same access privileges.

When a role is assigned to an application or the definition of an item (a specific query, for example), only those Guardium users who are also assigned that role can access that component. If no security roles are assigned to a component (a report, for example), only the user who defined that component and the admin user can access it.

At installation time, Guardium is configured with a default set of roles and a default set of user accounts. The Guardium access manager can create new roles and modify existing roles as needed.

## Groups

Guardium supports the grouping of elements to simplify creating and managing policies and to clarify the presentation of reports.

Grouping can simplify the process of creating policy and query definitions. It is often useful to group elements of the same type, and grouping can make the presentation of information on reports more straightforward. Groups are used by all subsystems, and all users share a single set of groups.

For an example of grouping, assume that your company has 25 separate data objects containing sensitive employee information, and you need to report on all access to these items. You could formulate a very long query testing for each of the 25 items. Alternatively, you could define a single group called sensitive employee info containing those 25 objects. That way, in queries or policy rule definitions, you only need to test if an object is a member of that group.

An additional benefit of groups is that they can ease maintenance requirements when the group's composition changes. To continue the example, if your company decides that two more objects need to be added to the sensitive employee info group, you only need to update the group definition and not all of the queries, reports, and policies that reference the group.

## Data archive and purge

Data Archive backs up data that has been captured by a Guardium system. When configuring Data Archive, data purge criteria may also be specified.

There are two archive operations: Data Archive and Results Archive. The path to these archive operations is Manage > Data Management > Data Archive or Results Archive (Audit).

### Data Archive

With Data Archive, data is typically archived at the end of the day on which it is captured, which ensures that in the event of a catastrophe, only the data of that day is lost. The purging of data depends on the application and depends on business and auditing requirements, but in most cases data can be kept on the machines for more than six months.

### Results Archive

Results Archive backs up audit task results (e.g. reports, assessment tests, entity audit trail, privacy sets, and classification processes) as well as the view and sign-off trails and the accommodated comments from workflow processes. Results sets are purged from the system according to the workflow process definition.

In an aggregation environment, data can be archived from the collector, from the aggregator, or from both locations. Most commonly, the data is archived only once, and the location from where it is archived varies depending on the customer's requirements.

Purge is enabled by default, at a 60 day interval.

## Related tasks

- [Managing stored data](#)
- [Purging data](#)

## Guardium Installation Manager

The Guardium Installation Manager (GIM) is used to install and maintain Guardium components on managed systems.

The GIM component includes a GIM server, which is installed as part of the Guardium system, and a GIM client, which must be installed on servers that host databases and file servers you want to monitor. After installing the GIM client, it works with the GIM server to perform the following tasks:

- Check for updates to installed software
- Transfer and install new software
- Uninstall software
- Update software parameters

If your environment includes a Guardium system configured as a Central Manager, you must decide which Guardium systems you want to use as GIM servers. You can either manage all of your GIM clients from a single Guardium system, such as the central manager, or you can manage them in groups from the different Guardium systems. If you manage all of your GIM clients from a single Guardium system, then you can view the status of all the GIM clients and perform related tasks from a single interface. If you choose to manage your GIM clients in groups from separate Guardium systems, then you can use each system to work with the GIM clients that it manages, but no overall or environment-wide view is available.

## Discover

Discovery refers to processes of locating and identifying objects in your environment that must be tracked for security and compliance purposes.

Discovery is the process of finding important objects such as privileged users, sensitive data, and datasources. Classification is the process of appropriately identifying what is discovered for security and compliance purposes. These processes of discovery and classification are important in large organizations where mergers, acquisitions, and legacy systems introduce new objects to your environment in unstructured or unpredictable ways. GuardiumGuardium® helps you incorporate these objects into your environment so you can enforce effective security policies and ensure compliance.

A common scenario involves the discovery of sensitive data. Sensitive data refers to regulated information like credit card numbers, personal financial data, social security numbers, and other information that requires special handling. Guardium supports two different approaches for discovering sensitive data: by using the Discover Sensitive Data workflow builder, or by using the Policy Builder with other Guardium tools. The Discover Sensitive Data workflow builder is intended as an all-inclusive tool for establishing discovery and classification processes for sensitive data. Use it to specify rules for discovery, define actions to take on discovered data, specify which data sources to scan, distribute reports, and run the workflow on an automated schedule. For more advanced users, the Policy Builder supports more granular discovery and classification rules that can be easily incorporated into existing processes and Guardium applications.

- [Datasources](#)

Datasources store information about your database or repository such as the type of database, the location of the repository, or credentials that might be associated with it. You must define a datasource in order to use it with Guardium applications.

- [Database Auto-discovery](#)

The Auto-Discovery application scans and probes your servers for open ports to prevent unknown or unwanted connections to your network. You can run auto-discovery processes on demand, or schedule the processes on a periodic basis.

- [Cloud database service protection](#)

Protect your cloud databases by using data activity stream monitoring or by using native audit.

- [Database discovered instances rules](#)

Use the Database Discovered Instances Rules UI from a central manager to determine how to manage inspection engines for discovered databases.

- [Classification](#)

Classification policies and processes define how Guardium discovers and treats sensitive data such as credit card numbers, social security numbers, and personal financial data.

- [Discover Sensitive Data](#)  
Create an end-to-end scenario for discovering and classifying sensitive data.
  - [Runtime sensitive-object identification](#)  
Runtime sensitive-object identification processes response data looking for predefined patterns that match personally-identifiable and other sensitive information.
  - [Regular Expressions](#)  
Regular expressions can be used to search traffic for complex patterns in the data.
  - [FAM discovery and classification in Windows and UNIX-Linux file servers](#)  
File activity discovery and classification ensures integrity and protection of sensitive data on UNIX-Linux and Windows file servers.
  - [File discovery and classification for NAS and SharePoint](#)  
File Discovery, Entitlement and Classification (FDEC) for NAS and SharePoint servers enables scanning for file entitlement and classification of sensitive data which may be related to regulatory laws (e.g., GDPR, HIPAA).
  - [Entitlement Optimization](#)  
Entitlement Optimization mediates between the role of the DBA in providing users the entitlements that are required to perform their jobs efficiently, and the role of Security in keeping entitlements as accurate and as minimal as possible to prevent system vulnerabilities.
- 

## Datasources

Datasources store information about your database or repository such as the type of database, the location of the repository, or credentials that might be associated with it. You must define a datasource in order to use it with Guardium® applications.

- [Creating a datasource definition](#)  
A datasource is a database connection that is created and configured for use with Guardium applications such as Vulnerability Assessment and classifier. A datasource can be created by using the Datasource Definitions tool or by creating and uploading a CSV file by using the Customer Uploads tool in the Guardium user interface. You can also create a datasource by using Guardium APIs.
  - [Creating a datasource group](#)  
A datasource group is a collection of datasources that you can act on as a single unit. You can specify a datasource group in most Guardium applications where you can specify a single datasource, such as security assessments, classification, and discovery scenarios. Create datasource groups from the Datasource Definitions page in the Guardium UI or by using Guardium APIs.
  - [Configuring your datasource](#)  
The configuration varies depending on the type of database you are using.
  - [Configuring custom properties for your datasources](#)  
Enrich your datasources by defining and assigning custom properties.
  - [Working with existing datasources](#)  
After you create a datasource definition, you can clone, modify, or delete the datasource.
  - [Reporting on datasources](#)  
Guardium provides reports on the datasources that are in your environment and any changes made to them.
  - [Defining a datasource using a service name](#)  
You can define a datasource that enables your users to connect to an Oracle database by using the service name by using a custom URL.
  - [Managing KDC definitions](#)  
If your datasource requires authentication using Kerberos, you can specify the information needed for Guardium to obtain a Kerberos ticket before making the connection.
  - [Managing datasource credentials with CyberArk](#)  
Guardium supports the CyberArk Application Password Provider, a robust solution to the numerous maintenance and security challenges that arise in managing passwords. Use CyberArk to securely store, provision, audit, and manage your Guardium datasource credentials.
  - [Managing datasource credentials with AWS Secrets Manager](#)  
Integrate your Guardium system with the Amazon Web Services (AWS) Secrets Manager to securely store, manage, rotate, and retrieve credentials for your datasources that use the Amazon Relational Database Service (RDS).
  - [Managing datasource credentials with HashiCorp](#)  
Integrate your Guardium system with HashiCorp to securely store, manage, rotate, and retrieve credentials for all supported datasources. You can configure your Guardium system to authenticate to the HashiCorp vault by using a username and password with no Transport Layer Security (TLS), server-side authentication with TLS, or client-side authentication with TLS. If you use client-side authentication with TLS, you must create and import a client signed certificate on all your systems such as the central manager and managed units, if any.
- 

## Creating a datasource definition

A datasource is a database connection that is created and configured for use with Guardium® applications such as Vulnerability Assessment and classifier. A datasource can be created by using the Datasource Definitions tool or by creating and uploading a CSV file by using the Customer Uploads tool in the Guardium user interface. You can also create a datasource by using Guardium APIs.

### Before you begin

Ensure that the Guardium user has the privileges that are necessary to access the database. To assign database access privileges to a user, the database administrator must download and run a set of scripts on the database server. For more information, see [Database privileges for vulnerability assessments and classification](#).

You can also create a datasource group for any applications that use datasources. A datasource group can be static (based on available datasources), or dynamic (based on criteria).

### About this task

Use the following procedure to define a datasource by using the Datasource Definitions tool.

### Procedure

1. Open the Datasource Definitions tool by clicking **Setup > Tools and Views > Datasource Definitions**.
2. Click the **Datasources** tab.
3. Click  to open the Create datasource window. The inputs vary depending on your choice of application, database type, and datasource.
4. Select an Application type.
5. Enter a unique name for the datasource.
6. From the Database type menu, select the database or type of file.
7. Select Share datasource to share the datasource definition across all Guardium applications. If the datasource is not shared, you can use the definition only with the selected application type.
8. The authentication protocol depends on your choice of Database type.
  - Select Use SSL and Import server SSL certificate. The Add certificate option is available to datasources that support mutual SSL authentication. The certificate for mutual SSL authentication is added after the datasource configuration is saved.
  - To use LDAP authentication, select LDAP and proceed with assigning datasource credentials.
  - For Kerberos, pick a predefined Kerberos configuration from the Kerberos config menu and enter the Realm and KDC server.  
Tip: To check whether a Kerberos configuration exists on the Guardium GUI, go to **Setup > Tools and Views > Kerberos Configuration**. To create a new Kerberos configuration that defines your KDC and Realm, click .

The login credentials must be a valid Kerberos user ID and password that is also used for certificate authority (CA). Test your Kerberos credentials to ensure that it can be used to log in to the Hive beeline command line.
9. Select the appropriate Credential type.
  - Choose Assign credentials to manually enter the User name and password for the datasource.
  - Choose External password to obtain your password from an external credential management system. Select your credential management application from the External password type menu.
  - If credentials are not assigned, choose None.
10. Configure the Host name/IP address, Port number, Database, Connection property, and Custom URL. If you use Configuration Auditing System (CAS), click the Advanced tab and configure the CAS database instance.  
Tip: The inputs vary depending on the type of database you are using. For more information, see [Configuring your datasource](#).
11. Optional: Click the Custom tab and select a property from a list of customized values to assign to the datasource. If the custom properties are not configured, you can temporarily save the datasource and assign the properties later. For more information, see [Configuring custom properties for your datasources](#).
12. Save the datasource and test the connection. If applicable, add the mutual SSL authentication certificate by using the Add certificate button.  
The certificate is a PEM file that contains both the private key and the certificate. You must include both the BEGIN and END lines for the private key and certificate. You can also install the certificate by using the CLI. For more information, see [Installing an appliance certificate](#).  
Note: When you test the connection to an SSL datasource for the first time, you might encounter the following error:

```
Could not connect to: 'jdbc:db2://hostname:port_number/db_name' for user: 'Your_datasource_name_DB2(Security Assessment)'. DataSourceConnectException: Could not connect to: 'Your_datasource_name_123.123.123.123:port_number' for user: 'db2inst1'. Exception: com.ibm.db2.jcc.am.DisconnectNonTransientConnectionException: [jcc][t4][2030][11211] [4.15.134] A communication error occurred during operations on the connection's underlying socket, socket input stream.
```

The error occurs when the GUI does not have the correct keystore file for the certificate that is loaded into memory. To fix the error, restart the GUI and test the connection again.

## What to do next

You can use the options in the menu to test the connection for one or more datasources, add the datasources to a group, and update the credentials or custom properties, if necessary.

## Related concepts

- [Managing datasource credentials with CyberArk](#)

## Related tasks

- [Managing datasource credentials with AWS Secrets Manager](#)
- [Managing datasource credentials with HashiCorp](#)
- [Configuring custom properties for your datasources](#)

## Related information

- [Create or update datasources by uploading a CSV file](#)
- [LDAP import into custom tables](#)

## Creating a datasource group

A datasource group is a collection of datasources that you can act on as a single unit. You can specify a datasource group in most Guardium® applications where you can specify a single datasource, such as security assessments, classification, and discovery scenarios. Create datasource groups from the Datasource Definitions page in the Guardium UI or by using Guardium APIs.

## Before you begin

Make sure that you have the necessary privileges to access the database.

## About this task

Use the following procedure to define a datasource group from the Datasource Definitions page.

## Procedure

---

1. From the Guardium UI, browse to Setup > Tools and Views > Datasource Definitions.

2. Click the Datasource groups tab.

When you open the tab, the table is always populated with the All datasources group.

To view the datasources in any group, click the  icon in the Group name column.

3. Click  to open the Create group window.

Note: From Datasource groups, you can select an existing datasource group and click  to clone the datasource group. The copy of the selected group opens in the Create group window.

4. Enter a name for the new group.

5. Select the Group type

- Datasources based on criteria - Specify criteria to find existing datasources to include in the group. Use the dropdown lists to select the datasources for your group based on Datasource type, Application type, and Severity. You can also specify a User name or Host name/IP to narrow the datasources to include in this group.
- Selected datasources - Select existing datasources from the Available Datasources table.

- From the Available Datasources table, you can take the following actions:

- Click  to create a new datasource.
- Select a datasource and click  to update that datasource.
- Use the Filter box to filter on the datasource name, type, hostname or IP address, or username.
- Select the datasources that you want to include in the group. You can select the checkbox in the table heading to select all available datasources. If you created a filter, only the filtered datasources are selected.

- After you create the list of datasources for your group, click  to move the selected list to the Selected Datasources table.

6. Optionally, click Roles to assign one or more roles to this group.

7. When you are done, click Save to save your group.

## What to do next

---

You can specify a datasource group in most Guardium applications that accept datasources, including classification and Vulnerability Assessments (VA). You can edit or copy any existing datasource group, including the All datasources group.

You can also create and manage datasource groups by using GrdAPIs or REST APIs. The datasource group APIs all contain the words **datasource\_groupRef** in their name.

## Related information

---

- [Datasource group APIs](#)

## Configuring your datasource

---

The configuration varies depending on the type of database you are using.

Click the database type to see the configuration information for your datasource.

- [\*\*Amazon DynamoDB\*\*](#)  
12.1 and later Configure an Amazon DynamoDB datasource on your Guardium system.
- [\*\*Amazon Redshift\*\*](#)  
Configure an Amazon Redshift datasource on your Guardium system.
- [\*\*Apache Cassandra\*\*](#)  
Configure an Apache Cassandra datasource on your Guardium system.
- [\*\*Aster\*\*](#)  
Configure an Aster datasource on your Guardium system.
- [\*\*Cloudera Manager\*\*](#)  
Configure a Cloudera Manager datasource on your Guardium system.
- [\*\*CockroachDB\*\*](#)  
12.1 and later Configure a CockroachDB datasource on your Guardium system.
- [\*\*Couchbase\*\*](#)  
Configure a Couchbase datasource on your Guardium system.
- [\*\*DataStax Cassandra\*\*](#)  
Configure a DataStax Cassandra datasource with DataDirect connection on your Guardium system.
- [\*\*Db2\*\*](#)  
Configure a Db2® datasource on your Guardium system.
- [\*\*Db2 for i\*\*](#)  
Configure a Db2 for i datasource on your Guardium system.
- [\*\*Db2 for z/OS\*\*](#)  
Configure a Db2 for z/OS® datasource on your Guardium system.
- [\*\*EDB PostgreSQL\*\*](#)  
Configure an EnterpriseDB PostgreSQL datasource on your Guardium system.
- [\*\*GreenplumDB\*\*](#)  
Configure a GreenplumDB datasource on your Guardium system.

- [\*\*Guardium Big Data Intelligence\*\*](#)  
Configure a Guardium Big Data Intelligence (GBDI) datasource on your Guardium system.
- [\*\*Hive\*\*](#)  
Configure a Hive datasource on your Guardium system.
- [\*\*Informix\*\*](#)  
Configure an Informix® datasource on your Guardium system.
- [\*\*MariaDB\*\*](#)  
Configure a MariaDB datasource on your Guardium system.
- [\*\*MongoDB\*\*](#)  
Configure a MongoDB datasource on your Guardium system.
- [\*\*MS SQL Server \(DataDirect - Dynamic Port\)\*\*](#)  
Configure an MS SQL Server DataDirect - dynamic port datasource on your Guardium system.
- [\*\*MS SQL Server \(DataDirect\)\*\*](#)  
Configure an MS SQL Server DataDirect datasource on your Guardium system.
- [\*\*MS SQL Server \(Microsoft - Dynamic Port\)\*\*](#)  
Configure an MS SQL Server Microsoft - dynamic port datasource on your Guardium system.
- [\*\*MS SQL Server \(Microsoft\)\*\*](#)  
Configure an MS SQL Server Microsoft datasource on your Guardium system.
- [\*\*MySQL\*\*](#)  
Configure a MySQL datasource on your Guardium system.
- [\*\*Neo4j\*\*](#)  
Configure a Neo4j datasource on your Guardium system.
- [\*\*Netezza\*\*](#)  
Configure a Netezza® datasource on your Guardium system.
- [\*\*Oracle \(Data Direct - Service Name\)\*\*](#)  
Configure an Oracle datasource with DataDirect connection on your Guardium system.
- [\*\*Oracle \(Data Direct - SID\)\*\*](#)  
Configure an Oracle datasource with DataDirect connection on your Guardium system.
- [\*\*Percona MySQL\*\*](#)  
Configure a Percona MySQL datasource on your Guardium system.
- [\*\*PostgreSQL\*\*](#)  
Configure a PostgreSQL datasource on your Guardium system.
- [\*\*SAP HANA\*\*](#)  
Configure a SAP HANA datasource on your Guardium system.
- [\*\*Snowflake\*\*](#)  
Configure a Snowflake datasource on your Guardium system.
- [\*\*SQL DB Azure\*\*](#)  
Configure an SQL DB Azure datasource on your Guardium system.
- [\*\*Sybase\*\*](#)  
Configure a Sybase datasource on your Guardium system.
- [\*\*Sybase IQ\*\*](#)  
Configure a Sybase IQ datasource on your Guardium system.
- [\*\*TERADATA\*\*](#)  
Configure a TERADATA datasource on your Guardium system.
- [\*\*Text datasources\*\*](#)  
Parameters to configure a text datasource.

## Amazon DynamoDB

12.1 and later Configure an Amazon DynamoDB datasource on your Guardium® system.

### Supported Authentication Methods

| AWS Authentication   | Supported |
|----------------------|-----------|
| Security Credentials | Yes       |
| IAM role             | Yes       |
| IAM instance profile | Yes       |

Note: To set up and configure the AWS authentication type for your Guardium datasource, see [Selecting the authentication type and setting up roles](#).

### Parameters

| Field                            | Description                                                                                           |
|----------------------------------|-------------------------------------------------------------------------------------------------------|
| AWS authentication configuration | Required. The name of the AWS authentication configuration.                                           |
| Region                           | Required. The location of your data center region that is configured on your AWS management console.. |

## Amazon Redshift

Configure an Amazon Redshift datasource on your Guardium® system.

### Supported Authentication Methods

| <b>Authentication</b> | <b>Supported</b> |
|-----------------------|------------------|
| Local user            | Yes              |
| LDAP                  | No               |
| Kerberos              | No               |
| SSL                   | Yes              |
| Mutual SSL            | No               |

Note:

SSL certificates are included with the JDBC driver that Guardium uses to connect to Amazon Redshift. The default authentication method is SSL.

## Parameters

| <b>Field</b>        | <b>Description</b>                                                                                                                                                                                                                                                                               |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname of the datasource.                                                                                                                                                                                                                                                        |
| Port number         | Required. Default value: 5439                                                                                                                                                                                                                                                                    |
| Database            | The name of the database.                                                                                                                                                                                                                                                                        |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation. |

## Apache Cassandra

Configure an Apache Cassandra datasource on your Guardium® system.

Note: To use this feature, you must install the latest Guardium Vulnerability Assessment patch for version 11.5.

## Supported Authentication Methods

| <b>Authentication</b> | <b>Supported</b> |
|-----------------------|------------------|
| Local user            | Yes              |
| LDAP                  | No               |
| Kerberos              | No               |
| SSL                   | Yes              |
| Mutual SSL            | Yes              |

## Parameters

| <b>Field</b>        | <b>Description</b>                                                                                                                                                                                                                                                                               |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                          |
| Port number         | Required. Default value: 9042.                                                                                                                                                                                                                                                                   |
| Database            | The name of the database.                                                                                                                                                                                                                                                                        |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                        |

## CAS (Configuration Auditing System) database instance

If you are a CAS user, configure the CAS database instance.

| <b>Field</b> | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account      | The name of the account owner.<br>Example: cassandra                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Directory    | The name of the installation directory.<br>Define pipe separated variables for all Apache Cassandra datasources that run CAS scripts or templates.<br><br>Example:<br><code>/home/cassandra   installpath=/home/cassandra/apache-cassandra-4.x   logpath=/home/cassandra/apache-cassandra-4.x/log   CASSANDRA_CONF_PATH=/home/cassandra/apache-cassandra-4.x/conf</code><br><br>Where: <ul style="list-style-type: none"><li>• home/cassandra : is the home directory path for the Cassandra user. This entry is required.</li><li>• installpath=/home/cassandra/apache-cassandra-4.x : is the Red Hat Package Manager (RPM) default installation location. For .tar files, use the path to the folder where Apache Cassandra was extracted.</li><li>• logpath=/home/cassandra/apache-cassandra-4.x/log : is the default path to the log file. This path can be modified.</li><li>• CASSANDRA_CONF_PATH=/home/cassandra/apache-cassandra-4.x/conf : is the default RPM location of the configuration file. The default .tar file path is \$installpath/conf.</li></ul> |

## Related information

---

- [Troubleshooting Cassandra](#)

## Aster

Configure an Aster datasource on your Guardium® system.

### Supported Authentication Methods

---

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | No        |
| Kerberos       | No        |
| SSL            | No        |
| Mutual SSL     | No        |

### Parameters

---

| Field               | Description                                                                                                                                                                                                                                                                                      |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                          |
| Port number         | Required. Default value: 2406.                                                                                                                                                                                                                                                                   |
| Database            | The name of the database.<br>Example: beehive                                                                                                                                                                                                                                                    |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                        |

## CAS (Configuration Auditing System) database instance

---

If you are a CAS user, configure the CAS database instance.

| Field     | Description                                                       |
|-----------|-------------------------------------------------------------------|
| Account   | The name of the account owner.<br>Example: beehive                |
| Directory | The name of the installation directory.<br>Example: /home/beehive |

## Cloudera Manager

---

Configure a Cloudera Manager datasource on your Guardium® system.

### Supported Authentication Methods

---

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | Yes       |
| Kerberos       | No        |
| SSL            | Yes       |
| Mutual SSL     | No        |

### Parameters

---

| Field               | Description                                                                                                                                                                                    |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                        |
| Port number         | Required. Default value: 7184.                                                                                                                                                                 |
| Cluster name        | Required. The display name of the Cluster in the Cloudera Manager GUI.                                                                                                                         |
| Connection property | Properties that must be included to establish a connection with the datasource.<br>The Cloudera Manager datasource uses the Cloudera Manager Java™ API for a connection. It does not use JDBC. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                      |

## CAS (Configuration Auditing System) database instance

---

If you are a CAS user, configure the CAS database instance.

| Field     | Description                                                                   |
|-----------|-------------------------------------------------------------------------------|
| Account   | The name of the account owner.<br>Example: root                               |
| Directory | The name of the installation directory.<br>Example: installpath=/opt/cloudera |

---

## CockroachDB

12.1 and later Configure a CockroachDB datasource on your Guardium® system.

### Supported Authentication Methods

---

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | No        |
| Kerberos       | No        |
| SSL            | Yes       |
| Mutual SSL     | No        |

## Parameters

---

| Field               | Description                                                                                                                                                                                                                                                                                      |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                          |
| Port number         | Required. Default value: 26257.                                                                                                                                                                                                                                                                  |
| Database            | Required. The name of the database.<br>For example, defaultdb.<br>For Vulnerability Assessment (VA) tests that require scanning other databases, the VA assessment scan will get a list of all required databases from the CockroachDB instance and run the test.                                |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                        |

---

## Couchbase

Configure a Couchbase datasource on your Guardium® system.

You must configure one datasource per Couchbase instance.

### Supported Authentication Methods

---

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | Yes       |
| Kerberos       | No        |
| SSL            | No        |
| Mutual SSL     | Yes       |

## Steps to create, configure, and import the SSL client certificate into your Guardium system

---

1. Use the Couchbase online documentation to setup Couchbase Server's support of X.509 certificates.
2. When you configure the server certificates, create a customized certificate extensions file, which adds the node constraints to the generic constraints that are already specified. Add both IP and DNS with hostname to the `subjectAltName` to avoid getting an error. For example: `echo "subjectAltName = IP:9.42.32.60,DNS:dba-informix02.rtp.raleigh.ibm.com" \>> ./server.ext.tmp.`
3. Use the Couchbase online documentation to create an SSL client certificate to import into your Guardium system. The SSL client certificate must contain the client certificate and its private key.
4. Create an SSL Datasource on your Guardium system.

## Parameters

---

| Field        | Description                                             |
|--------------|---------------------------------------------------------|
| Host Name/IP | Required. The hostname or IP address of the datasource. |

| Field               | Description                                                                                                                                                                                                                                                                                                                                                  |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port number         | Required. Default value: 8091<br>When you connect using custom ports, use the externally visible ports on the client side.<br><br>For cluster manager ports, enter the custom port number.<br><br>For custom query service port (kv port) enter the custom value in the Connection property field by using the format in this example:<br>customKvPort=11214 |
| Database            | The name of the database.<br><br>If LDAP authentication is used, specify a valid bucket name for the database.<br>Note: All the Couchbase vulnerability assessment tests are configuration tests and privilege tests. The tests do not scan or access any data that's stored in a bucket.                                                                    |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation.                                                             |

## CAS (Configuration Auditing System) database instance

If you are a CAS user, configure the CAS database instance.

| Field     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account   | For the default installation of Couchbase, enter the "root" user. For a non-root or non-sudo installation, enter the OS user account.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Directory | The name of the installation directory.<br>You can specify multiple paths for the database instance directory. Indicate a separate path by using a pipe " " with spaces.<br><br>For example:<br>/root installpath=opt/couchbase.<br><br>Where:<br>/root is the instance account directory.<br>installpath=opt/couchbase is the installation directory.<br><br>When you install Couchbase with an RPM package, you must have root or sudo privileges. It is likely that the home directory of root user /root is the instance account directory. For a non-root or non-sudo installation, the instance account directory is the home directory of the OS user account under which Couchbase is installed.<br><br>When you install Couchbase with an RPM package, the installation directory is /opt/couchbase by default. For a non-root or non-sudo installation, enter the path to the installation location. For example: /home/cb651/cb/opt/couchbase. |

## DataStax Cassandra

Configure a DataStax Cassandra datasource with DataDirect connection on your Guardium® system.

## Supported Authentication Methods

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | Yes       |
| Kerberos       | No        |
| SSL            | Yes       |
| Mutual SSL     | Yes       |

## Parameters

| Field               | Description                                                                                                                                                                                                                                                                                      |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                          |
| Port number         | Required. Default value: 9042.                                                                                                                                                                                                                                                                   |
| Database            | The name of the database.                                                                                                                                                                                                                                                                        |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                        |

## CAS (Configuration Auditing System) database instance

If you are a CAS user, configure the CAS database instance.

| Field | Description |
|-------|-------------|
|       |             |

| Field     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account   | The name of the account owner.<br>Example: <code>cassandra</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Directory | The name of the installation directory.<br>Define pipe separated variables for all DSE Cassandra datasources that run CAS scripts or templates.<br><br>Example:<br><br><code>/var/lib/cassandra   installpath=/var/lib/cassandra   logpath=/var/log/cassandra   compath=/usr/share/dse   CASSANDRA_CONF_PATH=/etc/dse/cassandra   DSE_CONF_PATH=/etc/dse</code><br><br>Where: <ul style="list-style-type: none"> <li>• <code>/var/lib/cassandra</code> Is the home directory path for the Cassandra user. This entry is required.</li> <li>• <code>installpath=/var/lib/cassandra</code> Is the Red Hat Package Manager (RPM) default installation location. For .tar files, use the path to the folder where DataStax Enterprise was extracted.</li> <li>• <code>logpath=/var/log/cassandra</code> Is the default path to the log file. This path can be modified.</li> <li>• <code>compath=/usr/share/dse</code> Is the default RPM path to the location of the components. The components are DSE Analytics, DSEFS, DSE Search, DSE Graph, DSE Advanced Replication, DSE In-Memory, DSE Multi-Instance, DSE Tiered Storage and DSE Performance services. The default .tar file path is <code>\$installpath/resources</code>.</li> <li>• <code>CASSANDRA_CONF_PATH=/etc/dse/cassandra</code> Is the default RPM location of the configuration file. The default .tar file path is <code>\$installpath/resources/cassandra/conf</code>.</li> <li>• <code>DSE_CONF_PATH=/etc/dse</code> Is the default RPM location. The default .tar file path is <code>\$installpath/resources/dse/conf</code>.</li> </ul> |

## Related information

- [Troubleshooting Cassandra](#)

## Db2

Configure a Db2® datasource on your Guardium® system.

## Supported Authentication Methods

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | No        |
| Kerberos       | No        |
| SSL            | Yes       |
| Mutual SSL     | No        |

## Parameters

| Field               | Description                                                                                                                                                                                                                                                                                                    |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                                        |
| Database name       | The name of the database.                                                                                                                                                                                                                                                                                      |
| Port number         | Required. Default value: <code>50000</code> .                                                                                                                                                                                                                                                                  |
| Schema              | The name of the database schema.                                                                                                                                                                                                                                                                               |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is <code>property1=value;property2=value</code> , where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.<br>Example: For an encrypted connection, enter <code>securityMechanism=13</code>                                                     |

## CAS (Configuration Auditing System) database instance

If you are a CAS user, configure the CAS database instance.

| Field     | Description                                                                                                                                                                                                                                          |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account   | The name of the account owner.<br>Example: <code>db2inst1</code>                                                                                                                                                                                     |
| Directory | The name of the installation directory.<br>Usually the home directory of db2inst1 or C:\Program Files\IBM\SQLLIB on Windows<br><br>The program db2cmd.exe must be on the system path, or in the bin subdirectory of the Database Instance Directory. |

## Db2 for i

Configure a Db2® for i datasource on your Guardium® system.

## Supported Authentication Methods

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | No        |
| Kerberos       | No        |
| SSL            | No        |
| Mutual SSL     | No        |

## Parameters

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Port number         | Required. Default value: 446.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Service name        | The service name of the database.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Schema              | The name of the database schema.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation.<br><br>When a password is due to expire, a warning prompt appears 7 days before the expiration date. This expiration message might cause the login to fail. To avoid this scenario, add <code>prompt=false</code> to the connection properties. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.<br>Example: <code>property1=com.ibm.as400.access.AS400JDBCDriver;translate binary=true</code>                                                                                                                                                                                                                                                                          |

## Db2 for z/OS

Configure a Db2® for z/OS® datasource on your Guardium® system.

## Prerequisite

Download and install the Db2 for z/OS JDBC license file from Passport Advantage. For more information, see [Uploading a JDBC license file for mainframe hosts to the Guardium system](#).

## Supported Authentication Methods

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | No        |
| Kerberos       | No        |
| SSL            | Yes       |
| Mutual SSL     | Yes       |

## Parameters

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                                                                                                        |
| Location name       | Required. The location of the database.                                                                                                                                                                                                                                                                                                                                        |
| Port number         | Required. Default value: 446.                                                                                                                                                                                                                                                                                                                                                  |
| Schema              | The name of the database schema.                                                                                                                                                                                                                                                                                                                                               |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation.<br>To enhance database performance, enter <code>resultSetHoldability=2</code> |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                                                                                                      |

## EDB PostgreSQL

Configure an EnterpriseDB PostgreSQL datasource on your Guardium® system.

## Supported Authentication Methods

| <b>Authentication</b> | <b>Supported</b> |
|-----------------------|------------------|
| Local user            | Yes              |
| LDAP                  | No               |
| Kerberos              | No               |
| SSL                   | Yes              |
| Mutual SSL            | Yes              |

## Parameters

| <b>Field</b>        | <b>Description</b>                                                                                                                                                                                                                                                                               |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                          |
| Port number         | Required. Default value: 5432.                                                                                                                                                                                                                                                                   |
| Database            | Required. The name of the database.<br>For example, postgres.<br>For Vulnerability Assessment (VA) tests that require scanning other databases, the VA assessment scan will get a list of all required databases from the EDB PostgreSQL instance and run the test.                              |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                        |

## CAS (Configuration Auditing System) database instance

If you are a CAS user, configure the CAS database instance.

| <b>Field</b> | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account      | The name of the account owner.<br>Example: enterpriseedb                                                                                                                                                                                                                                                                                                                                                                                                          |
| Directory    | The name of the installation directory.<br>You can specify multiple paths for the database instance directory. Indicate a separate path by using a pipe " " with a space before and after the delimiter.<br><br>For example: /var/lib/edb   PostgreSQL_DATA=/var/lib/edb/as14/data<br><br>Note: PostgreSQL_DATA should be the same path as the PGDATA environment variable. It is the data directory from where the EDB PostgreSQL cluster (instance) is running. |

## GreenplumDB

Configure a GreenplumDB datasource on your Guardium® system.

## Supported Authentication Methods

| <b>Authentication</b> | <b>Supported</b> |
|-----------------------|------------------|
| Local user            | Yes              |
| LDAP                  | No               |
| Kerberos              | No               |
| SSL                   | No               |
| Mutual SSL            | No               |

## Parameters

| <b>Field</b>        | <b>Description</b>                                                                                                                                                                                                                                                                               |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                          |
| Port number         | Required. Default value: 5432.                                                                                                                                                                                                                                                                   |
| Database            | Required. The name of the database.                                                                                                                                                                                                                                                              |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                        |

## Guardium Big Data Intelligence

Configure a Guardium® Big Data Intelligence (GBDI) datasource on your Guardium system.

## Supported Authentication Methods

---

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | Yes       |
| Kerberos       | Yes       |
| SSL            | Yes       |
| Mutual SSL     | Yes       |

## Parameters

---

| Field               | Description                                                                                                                                                               |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                   |
| Port number         | Required. Default value: 27117.                                                                                                                                           |
| Database            | The name of the database.                                                                                                                                                 |
| Connection property | Properties that must be included to establish a connection with the datasource.                                                                                           |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number. |

## Hive

---

Configure a Hive datasource on your Guardium® system.

To set up a Hive datasource, use the Apache Hive JDBC driver 1.1.1.

## Supported Authentication Methods

---

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | Yes       |
| Kerberos       | Yes       |
| SSL            | Yes       |
| Mutual SSL     | No        |

## Parameters

---

| Field               | Description                                                                                                                                                                                                                                                                                      |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                          |
| Port number         | Required. Default value: 10000.                                                                                                                                                                                                                                                                  |
| Database            | The name of the database.                                                                                                                                                                                                                                                                        |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                        |

## CAS (Configuration Auditing System) database instance

---

If you are a CAS user, configure the CAS database instance.

| Field     | Description                                                                   |
|-----------|-------------------------------------------------------------------------------|
| Account   | The name of the account owner.<br>Example: root                               |
| Directory | The name of the installation directory.<br>Example: installpath=/opt/cloudera |

## Informix

---

Configure an Informix® datasource on your Guardium® system.

## Supported Authentication Methods

---

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | No        |

| Authentication | Supported |
|----------------|-----------|
| Kerberos       | No        |
| SSL            | No        |
| Mutual SSL     | No        |

## Parameters

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Port number         | Required. Default value: 1526                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Informix server     | The name of the Informix server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Database            | The name of the database.<br>The default is sysmaster.<br><br>When the database name is sysmaster, the db_locale that is specified in the connection property field is used to connect to the sysmaster database.<br>For other databases, the db_locale in the sysdbslocale table is used.                                                                                                                                                                                                                                                                          |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation.<br><br>For Informix Unicode databases, the connection property <code>IFX_USE_STRENC=true</code> might be required.<br><br>Use the CLI command <code>store set_informix_driver_property</code> to set <code>IFX_USE_STRENC=true</code> on all Informix datasources. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                                                                                                                                                                                                                                                                                           |

## CAS (Configuration Auditing System) database instance

If you are a CAS user, configure the CAS database instance.

| Field     | Description                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account   | The name of the account owner.<br>Example: informix                                                                                                                                                                                                                                                                                                                                                         |
| Directory | The name of the installation directory.<br>On UNIX, the default is /opt/IBM/informix<br><br>On Windows, the default is C:\Program Files\IBM\Informix<br><br>An environment variable INFORMIXDIR can be defined.<br>The program <code>servicename.cmd</code> must be on the system path, where <code>servicename</code> is the name of the Informix server that is defined in the Datasource Definition GUI. |

## MariaDB

Configure a MariaDB datasource on your Guardium® system.

## Supported Authentication Methods

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | No        |
| Kerberos       | No        |
| SSL            | Yes       |
| Mutual SSL     | Yes       |

## Parameters

| Field               | Description                                                                                                                                                                                                                                                                                      |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                          |
| Database name       | The name of the database.                                                                                                                                                                                                                                                                        |
| Port number         | Required. Default value: 3306.                                                                                                                                                                                                                                                                   |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation. |

## CAS (Configuration Auditing System) database instance

If you are a CAS user, configure the CAS database instance.

| Field   | Description                    |
|---------|--------------------------------|
| Account | The name of the account owner. |

| Field     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Directory | <p>The name of the installation directory.<br/>An environment variable <i>MYSQL_HOME</i> may be defined.</p> <p>Example for rpm and yum installation: <i>MARIADB_HOME=/var/lib/mysql/</i></p> <p><i>MARIADB_HOME</i> (from MariaDB 10.6) is the environment variable that shows the path to the directory that contains the server-specific <i>my.cnf</i> file. If there is a <i>my.cnf</i> file in the MariaDB data directory but not in the MariaDB base directory, then <i>MARIADB_HOME</i> is set to the MariaDB data directory. Otherwise, <i>MARIADB_HOME</i> is set to the MariaDB base directory.</p> |

## MongoDB

Configure a MongoDB datasource on your Guardium® system.

### Supported Authentication Methods

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | Yes       |
| Kerberos       | Yes       |
| SSL            | Yes       |
| Mutual SSL     | Yes       |

## Parameters

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Port number         | Required. Default value: 27017.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Database            | The name of the database.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Connection property | <p>Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is <i>property1=value;property2=value</i>, where each property and value pair is separated by a semicolon.</p> <p>For examples, refer to the database vendor's JDBC documentation.</p> <p>Example:</p> <ul style="list-style-type: none"> <li>• <i>streamTypenio2 netty</i>: The stream type to use for connections. If unspecified, nio2 is used.</li> <li>• <i>sslInvalidHostNameAllowed=true false</i>: Specify whether invalid hostnames for SSL are allowed or not.</li> <li>• <i>connections.connectTimeoutMS=ms</i>: How long a connection takes to be open before it times out.</li> <li>• <i>socketTimeoutMS=ms</i>: How long a send or receive on a socket takes before it times out.</li> <li>• <i>maxIdleTimeMS=ms</i>: Maximum idle time of a pooled connection. A connection that exceeds this limit is closed.</li> <li>• <i>maxLifeTimeMS=ms</i>: Maximum life time of a pooled connection. A connection that exceeds this limit is closed.</li> </ul> |

## CAS (Configuration Auditing System) database instance

If you are a CAS user, configure the CAS database instance.

Important: To allow CAS scripts to run successfully as the *MONGOD* user, you must change the entry in */etc/passwd* from */bin/false* to */bin/bash*. By updating this file path, you can see data in the predefined CAS Saved Data report and avoid a potential No CAS Data result in your vulnerability assessment.

| Field     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account   | <p>The name of the account owner.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>• <i>mongodb</i></li> <li>• <i>mongos</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Directory | <p>The name of the installation directory.</p> <p>You can specify multiple paths for the database instance directory. Indicate a separate path by using a pipe "!" with spaces.</p> <p>For example, <i>/var/lib/mongo ! MongoBinary=/usr/bin ! dbpath=/var/lib/mongo ! logpath=/var/log/mongodb ! keytab=/home/keytab ! dbdumppath=/opt/backup ! sslpath=/etc/ssl ! keyfile=/home/mongod/mongo_server.keyfile</i>.</p> <p>Where:</p> <ul style="list-style-type: none"> <li>• <i>/var/lib/mongo</i> path is the home directory path for the MongoDB user. This entry is required.</li> <li>• <i>MongoBinary=/usr/bin</i> is the path to the MongoDB binary. The variable <i>MongoBinary</i> is case-sensitive.</li> <li>• <i>dbpath=/var/lib/mongo</i> is the path to the data files. In this example, it is the same as the MongoDB home directory.</li> <li>• <i>logpath=/var/log/mongodb</i> is the path to the MongoDB log.</li> <li>• <i>keytab=/home/keytab</i> is the directory to the MongoDB keytab file.</li> <li>• <i>dbdumppath=/opt/backup</i> is the directory to the MongoDB backup dump.</li> <li>• <i>sslpath=/etc/ssl</i> is the path to MongoDB SSL files.</li> <li>• <i>keyfile=/home/mongod/mongo_server.keyfile</i> points to the MongoDB keyfile.</li> </ul> <p>It is not required to define all the paths that are listed in this example. The paths that are not defined are not analyzed.</p> |

## MS SQL Server (DataDirect - Dynamic Port)

Configure an MS SQL Server DataDirect - dynamic port datasource on your Guardium® system.

The MS SQL Server DataDirect - dynamic port datasource can be used to connect dynamically to an MS SQL Server database when the dynamic function is enabled in the MS SQL Server database server. It can also be used to connect dynamically when a client does not have a defined port value.

### Supported Authentication Methods

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | Yes       |
| Kerberos       | No        |
| SSL            | Yes       |
| Mutual SSL     | No        |

### Parameters

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                                                                                                                                                                                    |
| Instance name       | The name of the instance to which you want to connect on the server.                                                                                                                                                                                                                                                                                                                                                                                       |
| Database            | The name of the database.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation.<br>Example: domain=domain_name;AuthenticationMethod=authentication_method;<br>encryptionMethod=encryption_method;validateServerCertificate=true_or_false. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                                                                                                                                                                                  |

### Adding custom properties for classification

To improve the performance of Guardium classification scans, you can add the following custom properties for Microsoft SQL Server.

- LARGE-TEXT-DATA-TYPE-MAX-LENGTH - By default, when scanning large data types like XML or VARCHAR(MAX), the classifier only samples the first 3000 characters. Use the LARGE-TEXT-DATA-TYPE-MAX-LENGTH property to define a custom length in the range of 0 - 2147483647 characters.
- MAXDOP - The MAXDOP property defines how many processors MS SQL Server uses for parallel plan execution. The default setting of 0 allows MS SQL Server to use all available processors (up to a maximum of 64). Setting MAXDOP to 1 prevents parallel plan generation. Allowed values are 0 - 32,767. For more information, see *Set the Max Degree of Parallelism Option* in the Microsoft SQL Docs.
- TRANSACTION-ISOLATION-LEVEL - When you add this property with *READ-UNCOMMITTED*, the classifier reads all rows (including uncommitted rows). *READ-UNCOMMITTED* is the only value currently supported for the TRANSACTION-ISOLATION-LEVEL property, and the value must be uppercase and include the hyphen. For more information, see *SET TRANSACTION ISOLATION LEVEL* in the Microsoft SQL Docs.

You can add or change custom properties from either the Guardium UI or by using GRDAPi commands. After you add the custom properties, the information displays in the Details for datasource output. For more information about adding custom properties from the UI, see [Configuring custom properties for your datasources](#).

You can use GRDAPi to manage custom properties. For example, use the following to create MAXDOP and TRANSACTION-ISOLATION-LEVEL custom properties:

```
grdapicreate_datasource_custom_property name=MAXDOP values=1
grdapicreate_datasource_custom_property name="TRANSACTION-ISOLATION-LEVEL" values="READ-UNCOMMITTED"
```

Use the following to add the MAXDOP and TRANSACTION-ISOLATION-LEVEL properties to a MS SQL Server datasource:

```
grdapicreate_datasource_by_name customProps="TRANSACTION-ISOLATION-LEVEL=READ-UNCOMMITTED"
name="yourmssqlserverdatabasename"
grdapicreate_datasource_by_name customProps=MAXDOP=1 name="yourmssqlserverdatabasename"
```

Use the following to add additional MAXDOP values (where 2,4 indicates the list of values added):

```
grdapicreate_datasource_custom_property name=MAXDOP addValues=2,4
```

For more information about the custom property APIs, see [Datasource custom property APIs](#).

For more information about classification, see [Discover Sensitive Data](#).

### CAS (Configuration Auditing System) database instance

If you are a CAS user, configure the CAS database instance.

| Field   | Description                                                                |
|---------|----------------------------------------------------------------------------|
| Account | The name of the account owner. Required if Windows Authentication is used. |

| Field     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Directory | <p>The name of the installation directory.<br/>To use the datasource for Vulnerability Assessments, enter the path to your database instance home directory, for example,</p> <ul style="list-style-type: none"> <li>• MSSQL2014, default instance<br/>C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL</li> <li>• MSSQL2016, Name instance<br/>C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL</li> <li>• Oracle 2019<br/>C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL</li> <li>• Oracle 2022<br/>C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL</li> </ul> <p>To use the datasource for other tests such as CAS file monitoring, enter the path to the MS SQL Server directory, for example,</p> <ul style="list-style-type: none"> <li>• C:\Program Files (x86)\Microsoft SQL Server</li> <li>• C:\Program Files\Microsoft SQL Server</li> </ul> |

## MS SQL Server (DataDirect)

Configure an MS SQL Server DataDirect datasource on your Guardium® system.

Tip: To set a dynamic IP, go to the DB server and set the dynamic port type to 0. Remove TCP/IP and restart the services.

### Supported Authentication Methods

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | Yes       |
| Kerberos       | No        |
| SSL            | Yes       |
| Mutual SSL     | No        |

### Parameters

| Field         | Description                                                          |
|---------------|----------------------------------------------------------------------|
| Host Name/IP  | Required. The hostname or IP address of the datasource.              |
| Port number   | Required. Default value: 1433.                                       |
| Instance name | The name of the instance to which you want to connect on the server. |
| Database      | The name of the database. The default value is <i>Master</i> .       |

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Connection property | <p>Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is <code>property1=value;property2=value</code>, where each property and value pair is separated by a semicolon.</p> <p>For examples, refer to the database vendor's JDBC documentation.</p> <p>For example,</p> <pre><code>domain=domain_name;AuthenticationMethod=authentication_method; encryptionMethod=encryption_method;validateServerCertificate=true_or_false;</code></pre> <p>Where:</p> <ul style="list-style-type: none"> <li>• <code>domain_name</code> is the name of the domain server. If the driver cannot determine the domain name, the connection fails and produces an error.</li> <li>• <code>AuthenticationMethod</code> determines the authentication method that the driver uses when a connection is established. If the authentication method is not supported by the database server, the connection fails and produces an error.</li> </ul> <p>The following values for <code>AuthenticationMethod</code> are valid:</p> <ul style="list-style-type: none"> <li>◦ <code>ntlm</code></li> <li>◦ <code>ntlmjava</code></li> <li>◦ <code>ntlm2java</code></li> </ul> <p>For Windows authentication, use the following property:</p> <pre><code>domain=domain_name;AuthenticationMethod=ntlmjava</code></pre> <p>To use NTLMv2 for Windows authentication, use the following property:</p> <pre><code>domain=domain_name;AuthenticationMethod=ntlm2java</code></pre> <p>Attention:</p> <ul style="list-style-type: none"> <li>◦ If you specify <code>AuthenticationMethod=ntlmjava</code> when the <code>LMCompatabilityLevel</code> is restricted to NTLMv2, an error is returned. When the <code>LMCompatabilityLevel</code> is restricted to NTLMv2, <code>AuthenticationMethod</code> must be set to <code>ntlm2java</code>.</li> <li>◦ If you specify <code>AuthenticationMethod=ntlmjava</code> or <code>AuthenticationMethod=ntlm2java</code>, you must also specify the name of the domain server that administers the database. You can specify the domain server by using the <code>domain</code> property. If the <code>domain</code> property is not specified, the driver tries to determine the domain server from the <code>user</code> property. If the driver cannot determine the domain server name, it returns an exception.</li> </ul> <ul style="list-style-type: none"> <li>• For nonstandard databases:</li> </ul> <p>If you are using a nonstandard database Unicode such as <code>Azeri_Cyrillic_100_CI_AS</code> or <code>Chinese_Hong_Kong_Stroke_90_CI_AS</code>, then add the following parameter to the connection property:</p> <pre><code>CodePageOverride=UTF-8</code></pre> <ul style="list-style-type: none"> <li>• For SSL authentication:</li> </ul> <p>To use SSL, add the following property,</p> <pre><code>encryptionMethod=SSL;validateServerCertificate=false</code></pre> <ul style="list-style-type: none"> <li>• Connecting to named instances:</li> </ul> <ul style="list-style-type: none"> <li>◦ Microsoft SQL Server 2000 and higher support multiple instances of a Microsoft SQL Server database that is running concurrently on the same server.</li> <li>◦ An instance is identified by an instance name. To connect to a named instance by using a connection URL, use the following URL format,</li> </ul> <pre><code>jdb:datadirect:sqlserver://server_name\\instance_name</code></pre> <p>Where:</p> <ul style="list-style-type: none"> <li>▪ <code>server_name</code> is the IP address or hostname of the server.</li> <li>▪ <code>instance_name</code> is the name of the instance to which you want to connect on the server.</li> </ul> <p>For example, the following connection URL connects to an instance named <code>instance1</code> on <code>server1</code>:</p> <pre><code>jdb:datadirect:sqlserver://server1\\instance1;User=test;Password=secret</code></pre> <p>Where the first backslash character (\) in <code>\\instance_name</code> is an escape character.</p> |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Adding custom properties for classification

To improve the performance of Guardium classification scans, you can add the following custom properties for Microsoft SQL Server.

- `LARGE-TEXT-DATA-TYPE-MAX-LENGTH` - By default, when scanning large data types like XML or `VARCHAR(MAX)`, the classifier only samples the first 3000 characters. Use the `LARGE-TEXT-DATA-TYPE-MAX-LENGTH` property to define a custom length in the range of 0 - 2147483647 characters.
- `MAXDOP` - The `MAXDOP` property defines how many processors MS SQL Server uses for parallel plan execution. The default setting of 0 allows MS SQL Server to use all available processors (up to a maximum of 64). Setting `MAXDOP` to 1 prevents parallel plan generation. Allowed values are 0 - 32,767. For more information, see *Set the Max Degree of Parallelism Option* in the Microsoft SQL Docs.
- `TRANSACTION-ISOLATION-LEVEL` - When you add this property with `READ-UNCOMMITTED`, the classifier reads all rows (including uncommitted rows). `READ-UNCOMMITTED` is the only value currently supported for the `TRANSACTION-ISOLATION-LEVEL` property, and the value must be uppercase and include the hyphen. For more information, see `SET TRANSACTION ISOLATION LEVEL` in the Microsoft SQL Docs.

You can add or change custom properties from either the Guardium UI or by using GRDAPi commands. After you add the custom properties, the information displays in the Details for datasource output. For more information about adding custom properties from the UI, see [Configuring custom properties for your datasources](#).

You can use GRDAPi to manage custom properties. For example, use the following to create MAXDOP and TRANSACTION-ISOLATION-LEVEL custom properties:

```
grdapicreate_datasource_custom_property name=MAXDOP values=
grdapicreate_datasource_custom_property name="TRANSACTION-ISOLATION-LEVEL" values="READ-UNCOMMITTED"
```

Use the following to add the MAXDOP and TRANSACTION-ISOLATION-LEVEL properties to a MS SQL Server datasource:

```
grdapi add_custom_property_to_datasource_by_name customProps="TRANSACTION-ISOLATION-LEVEL=READ-UNCOMMITTED"
name="yourmssqlserverdatabasename"
grdapi add_custom_property_to_datasource_by_name customProps=MAXDOP=1 name="yourmssqlserverdatabasename"
```

Use the following to add additional MAXDOP values (where **2,4** indicates the list of values added):

```
grdapi update_datasource_custom_property name=MAXDOP addValues=2,4
```

For more information about the custom property APIs, see [Datasource custom property APIs](#).

For more information about classification, see [Discover Sensitive Data](#).

## CAS (Configuration Auditing System) database instance

If you are a CAS user, configure the CAS database instance.

| Field     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account   | The name of the account owner. Required if Windows Authentication is used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Directory | <p>The name of the installation directory.<br/>To use the datasource for Vulnerability Assessments, enter the path to your database instance home directory, for example,</p> <ul style="list-style-type: none"><li>• MSSQL2014, default instance<br/>C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL</li><li>• MSSQL2016, Name instance<br/>C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL</li><li>• Oracle 2019<br/>C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL</li><li>• Oracle 2022<br/>C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL</li></ul> <p>To use the datasource for other tests such as CAS file monitoring, enter the path to the MS SQL Server directory, for example,</p> <ul style="list-style-type: none"><li>• C:\Program Files (x86)\Microsoft SQL Server</li><li>• C:\Program Files\Microsoft SQL Server</li></ul> |

## MS SQL Server (Microsoft - Dynamic Port)

Configure an MS SQL Server Microsoft - dynamic port datasource on your Guardium® system.

The MS SQL Server Microsoft - dynamic port datasource can be used to connect dynamically to an MS SQL Server database when the dynamic function is enabled in the MS SQL Server database server. It can also be used to connect dynamically when a client does not have a defined port value.

## Supported Authentication Methods

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | No        |
| Kerberos       | No        |
| SSL            | Yes       |
| Mutual SSL     | Yes       |

## Parameters

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Instance name       | The name of the instance to which you want to connect on the server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Database            | The name of the database.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation.<br>Example:<br><br>trustServerCertificate=true<br><br>If you are not using trustServerCertificate=true in your connection property, you must configure the server certificates with the CN and SAN so <b>hostNameInCertificate</b> or the <b>serverName</b> can be used in the connection property for TLS verification.<br>The value passed to <b>serverName</b> must match the Common Name (CN) or DNS name in the Subject Alternate Name (SAN) in the server certificate for a TLS connection to succeed. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## Adding custom properties for classification

---

To improve the performance of Guardium classification scans, you can add the following custom properties for Microsoft SQL Server.

- **LARGE-TEXT-DATA-TYPE-MAX-LENGTH** - By default, when scanning large data types like XML or VARCHAR(MAX), the classifier only samples the first 3000 characters. Use the LARGE-TEXT-DATA-TYPE-MAX-LENGTH property to define a custom length in the range of 0 - 2147483647 characters.
- **MAXDOP** - The MAXDOP property defines how many processors MS SQL Server uses for parallel plan execution. The default setting of 0 allows MS SQL Server to use all available processors (up to a maximum of 64). Setting MAXDOP to 1 prevents parallel plan generation. Allowed values are 0 - 32,767. For more information, see *Set the Max Degree of Parallelism Option* in the Microsoft SQL Docs.
- **TRANSACTION-ISOLATION-LEVEL** - When you add this property with *READ-UNCOMMITTED*, the classifier reads all rows (including uncommitted rows). *READ-UNCOMMITTED* is the only value currently supported for the TRANSACTION-ISOLATION-LEVEL property, and the value must be uppercase and include the hyphen. For more information, see *SET TRANSACTION ISOLATION LEVEL* in the Microsoft SQL Docs.

You can add or change custom properties from either the Guardium UI or by using GRDAPI commands. After you add the custom properties, the information displays in the Details for datasource output. For more information about adding custom properties from the UI, see [Configuring custom properties for your datasources](#).

You can use GRDAPIs to manage custom properties. For example, use the following to create MAXDOP and TRANSACTION-ISOLATION-LEVEL custom properties:

```
grdapi create_datasource_custom_property name=MAXDOP values=1
grdapi create_datasource_custom_property name="TRANSACTION-ISOLATION-LEVEL" values="READ-UNCOMMITTED"
```

Use the following to add the MAXDOP and TRANSACTION-ISOLATION-LEVEL properties to a MS SQL Server datasource:

```
grdapi add_custom_property_to_datasource_by_name customProps="TRANSACTION-ISOLATION-LEVEL=READ-UNCOMMITTED"
name="yourmssqlserverdatabasename"
grdapi add_custom_property_to_datasource_by_name customProps=MAXDOP=1 name="yourmssqlserverdatabasename"
```

Use the following to add additional MAXDOP values (where 2, 4 indicates the list of values added):

```
grdapi update_datasource_custom_property name=MAXDOP addValues=2,4
```

For more information about the custom property APIs, see [Datasource custom property APIs](#).

For more information about classification, see [Discover Sensitive Data](#).

## CAS (Configuration Auditing System) database instance

---

If you are a CAS user, configure the CAS database instance.

| Field     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account   | The name of the account owner. Required if Windows Authentication is used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Directory | <p>The name of the installation directory.<br/>To use the datasource for Vulnerability Assessments, enter the path to your database instance home directory, for example,</p> <ul style="list-style-type: none"><li>• MSSQL2014, default instance<br/>C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL</li><li>• MSSQL2016, Name instance<br/>C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL</li><li>• Oracle 2019<br/>C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL</li><li>• Oracle 2022<br/>C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL</li></ul> <p>To use the datasource for other tests such as CAS file monitoring, enter the path to the MS SQL Server directory, for example,</p> <ul style="list-style-type: none"><li>• C:\Program Files (x86)\Microsoft SQL Server</li><li>• C:\Program Files\Microsoft SQL Server</li></ul> |

## MS SQL Server (Microsoft)

---

Configure an MS SQL Server Microsoft datasource on your Guardium® system.

Tip: To set a dynamic IP, go to the DB server and set the dynamic port type to 0. Remove TCP/IP and restart the services.

## Supported Authentication Methods

---

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | Yes       |
| Kerberos       | No        |
| SSL            | Yes       |
| Mutual SSL     | No        |

## Parameters

---

| Field               | Description                                                                                                                                                                                                                                                                                   |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                       |
| Port number         | Required. Default value: 1433.                                                                                                                                                                                                                                                                |
| Instance name       | The name of the instance to which you want to connect on the server.                                                                                                                                                                                                                          |
| Database            | The name of the database. The default value is <i>Master</i> .                                                                                                                                                                                                                                |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon. For examples, refer to the database vendor's JDBC documentation. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                     |

## Adding custom properties for classification

To improve the performance of Guardium classification scans, you can add the following custom properties for Microsoft SQL Server.

- LARGE-TEXT-DATA-TYPE-MAX-LENGTH - By default, when scanning large data types like XML or VARCHAR(MAX), the classifier only samples the first 3000 characters. Use the LARGE-TEXT-DATA-TYPE-MAX-LENGTH property to define a custom length in the range of 0 - 2147483647 characters.
- MAXDOP - The MAXDOP property defines how many processors MS SQL Server uses for parallel plan execution. The default setting of 0 allows MS SQL Server to use all available processors (up to a maximum of 64). Setting MAXDOP to 1 prevents parallel plan generation. Allowed values are 0 - 32,767. For more information, see *Set the Max Degree of Parallelism Option* in the Microsoft SQL Docs.
- TRANSACTION-ISOLATION-LEVEL - When you add this property with *READ-UNCOMMITTED*, the classifier reads all rows (including uncommitted rows). *READ-UNCOMMITTED* is the only value currently supported for the TRANSACTION-ISOLATION-LEVEL property, and the value must be uppercase and include the hyphen. For more information, see *SET TRANSACTION ISOLATION LEVEL* in the Microsoft SQL Docs.

You can add or change custom properties from either the Guardium UI or by using GRDAPi commands. After you add the custom properties, the information displays in the Details for datasource output. For more information about adding custom properties from the UI, see [Configuring custom properties for your datasources](#).

You can use GRDAPi to manage custom properties. For example, use the following to create MAXDOP and TRANSACTION-ISOLATION-LEVEL custom properties:

```
grdapapi create_datasource_custom_property name=MAXDOP values=1
grdapapi create_datasource_custom_property name="TRANSACTION-ISOLATION-LEVEL" values="READ-UNCOMMITTED"
```

Use the following to add the MAXDOP and TRANSACTION-ISOLATION-LEVEL properties to a MS SQL Server datasource:

```
grdapapi add_custom_property_to_datasource_by_name customProps="TRANSACTION-ISOLATION-LEVEL=READ-UNCOMMITTED"
name="yourmssqlserverdatabasename"
grdapapi add_custom_property_to_datasource_by_name customProps=MAXDOP=1 name="yourmssqlserverdatabasename"
```

Use the following to add additional MAXDOP values (where 2, 4 indicates the list of values added):

```
grdapapi update_datasource_custom_property name=MAXDOP addValues=2,4
```

For more information about the custom property APIs, see [Datasource custom property APIs](#).

For more information about classification, see [Discover Sensitive Data](#).

## CAS (Configuration Auditing System) database instance

If you are a CAS user, configure the CAS database instance.

| Field     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account   | The name of the account owner. Required if Windows Authentication is used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Directory | <p>The name of the installation directory. To use the datasource for Vulnerability Assessments, enter the path to your database instance home directory, for example,</p> <ul style="list-style-type: none"> <li>MSSQL2014, default instance<br/>C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL</li> <li>MSSQL2016, Name instance<br/>C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL</li> <li>Oracle 2019<br/>C:\Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL</li> <li>Oracle 2022<br/>C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL</li> </ul> <p>To use the datasource for other tests such as CAS file monitoring, enter the path to the MS SQL Server directory, for example,</p> <ul style="list-style-type: none"> <li>C:\Program Files (x86)\Microsoft SQL Server</li> <li>C:\Program Files\Microsoft SQL Server</li> </ul> |

## MySQL

Configure a MySQL datasource on your Guardium® system.

## Supported Authentication Methods

Note: For SQL statements, the Guardium appliance supports UTF8 characters of up to 3 bytes in length. UTF8 characters 4 bytes or longer are not supported and do not display correctly. This is a limitation of the Guardium appliance.

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | No        |
| Kerberos       | No        |
| SSL            | Yes       |
| Mutual SSL     | Yes       |

## Parameters

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Port number         | Required. Default value: 3306.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Database            | The name of the database.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation.<br>If the database server is in the UTC time zone and you are unable to establish a connection, use the following connection properties:<br><code>useUnicode=true;useJDBCCompliantTimezoneShift=true;useLegacyDatetimeCode=false;serverTimezone=UTC</code> |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                                                                                                                                                                                                                                                                                   |

## CAS (Configuration Auditing System) database instance

If you are a CAS user, configure the CAS database instance.

| Field   | Description                    |
|---------|--------------------------------|
| Account | The name of the account owner. |

| Field     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Directory | <p>The name of the installation directory.<br/>An environment variable <code>MYSQL_HOME</code> may be defined.</p> <p>Note: A MySQL datasource with a Unicode database name is not supported. The datasource name in MySQL must be ASCII.<br/>To use the following feature, you must install the latest Guardium Vulnerability Assessment patch for version 11.5:</p> <p>Required environment variable:</p> <p><code>datadir</code> - The path to the MySQL server data directory. For MySQL Binary installation, the default path is <code>datadir=/usr/local/mysql/data</code>. For MySQL rpm or yum installation, the default path is <code>datadir=/var/lib/mysql</code></p> <p><code>MYSQL_HOME</code> is an environment variable containing the path to the directory in which the server-specific <code>my.cnf</code> file resides.</p> <p>If <code>MYSQL_HOME</code> is not set and you start the server using the <code>mysqld_safe</code> program, <code>mysqld_safe</code> sets it to <code>BASEDIR</code>, the MySQL base installation directory.</p> <p>If directories are not set to default, Optional variables can be set on the datasource CAS database instance Directory:</p> <p><code>\$log_bin_basename</code> - basename for the log bin files with full path (for example: <code>/var/lib/mysql/binlog</code>, will check for all log files starting with <code>binlog</code> under the <code>/var/lib/mysql</code> directory)</p> <p><code>\$slow_query_log_file</code> - slow query log file name with full path</p> <p><code>\$log_error</code> - Error log file name with full path</p> <p><code>\$general_log_file</code> - General log file name with full path</p> <p><code>\$relay_log_basename</code> - Basename for the relay logs files with full path (for example: <code>/var/lib/mysql/&lt;hostname&gt;-relay-bin.nnnnnn</code>)</p> <p><code>\$plugin_dir</code> - plugin dir with full path</p> <p><code>\$ssl_dir</code> - folder path where ssl key files are in with full path</p> <p><code>\$audit_log_file</code> - audit log file name with full path</p> <ul style="list-style-type: none"> <li>Example 1 - MySQL default installation with CAS instance OS account is <code>root</code>:<br/>Account: <code>root</code><br/>Directory: <code>/root / datadir=/var/lib/mysql</code></li> <li>Example 2 - MySQL binaries installation with CAS instance OS account is <code>mysql8c</code>:<br/>Account: <code>mysql8c</code><br/>Directory: <code>/home/mysql8c / datadir=/home/mysql8c/mysql/data/</code></li> <li>For example3 - MySQL installation with CAS instance OS account is <code>root</code> and non-default directories:<br/>Account: <code>root</code><br/>Directory: <code>/root / datadir=/opt/IBM/data/mysql/   slow_query_log_file=/opt/IBM/data/mysql/mysql-slow.log / log_error=/opt/IBM/data/mysql/mysql-error.log   general_log_file=/opt/IBM/data/mysql/localhost.log / relay_log_basename=/opt/IBM/data/mysql/localhost-relay-bin / ssl_dir=/opt/IBM/etc/keys</code></li> </ul> |

## Neo4j

Configure a Neo4j datasource on your Guardium® system.

## Supported Authentication Methods

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | No        |
| Kerberos       | No        |
| SSL            | Yes       |
| Mutual SSL     | Yes       |

## Parameters

| Field               | Description                                                                                                                                                                                                                                                                                                    |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                                        |
| Port number         | Required. Default value: 7687.                                                                                                                                                                                                                                                                                 |
| Database            | The name of the database.<br>Example: <code>system</code> .                                                                                                                                                                                                                                                    |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is <code>property1=value;property2=value</code> , where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation. |

| Field      | Description                                                                                                                                                               |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Custom URL | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number. |

## CAS (Configuration Auditing System) database instance

If you are a CAS user, configure the CAS database instance.

| Field     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account   | The name of the account owner.<br>For an RPM installation, the default account owner is <i>neo4j</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Directory | The name of the installation directory.<br>You can specify multiple paths for the database instance directory. Indicate a separate path by using a pipe " " with spaces.<br><br>For example:<br><code>/var/lib/neo4j   NEO4J_HOME=/var/lib/neo4j</code><br><br>Where: <ul style="list-style-type: none"> <li>• /var/lib/neo4j is the instance account directory.<br/>In an RPM (Red Hat Package Manager) installation, an OS user <i>neo4j</i> and an account directory path /var/lib/neo4j, is created by default. For .tar files, use the path to the home directory of the OS user account, under which Neo4j is installed.</li> <li>• NEO4J_HOME=/var/lib/neo4j is the Neo4j installation directory.<br/>In an RPM installation, the NEO4J_HOME directory is /var/lib/neo4j, by default. For .tar files, use the path to the folder where Neo4j is extracted.</li> </ul> |

## Netezza

Configure a Netezza® datasource on your Guardium® system.

## Supported Authentication Methods

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | No        |
| Kerberos       | No        |
| SSL            | No        |
| Mutual SSL     | No        |

## Parameters

| Field               | Description                                                                                                                                                                                                                                                                                      |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                          |
| Port number         | Required. Default value: 5480.                                                                                                                                                                                                                                                                   |
| Database            | The name of the database.                                                                                                                                                                                                                                                                        |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                        |

## CAS (Configuration Auditing System) database instance

If you are a CAS user, configure the CAS database instance.

| Field     | Description                                                                                                                       |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------|
| Account   | The name of the account owner.                                                                                                    |
| Directory | The name of the installation directory. This is not required as the Netezza installation is in the same location on all machines. |

## Oracle (Data Direct - Service Name)

Configure an Oracle datasource with DataDirect connection on your Guardium® system.

## Supported Authentication Methods

| Authentication | Supported |
|----------------|-----------|
|                |           |

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | Yes       |
| Kerberos       | No        |
| SSL            | Yes       |
| Mutual SSL     | Yes       |

## Parameters

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Port number         | Required. Default value: 1521                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Service name        | The service name of the database.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Schema              | The name of the database schema.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Connection property | <p>Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon. For examples, refer to the database vendor's JDBC documentation.</p> <p>The Oracle JDBC driver does not require a connection property. But the latest Oracle JDBC driver must be downloaded from Oracle. The filename is ojdbc7.jar. Search and download the open source JDBC drivers. For example: use the search query <a href="#">open source JDBC driver for Oracle</a>. Then upload the driver to the appliance using the Guardium Customer Uploads function.</p> <p>If you continue to use the Oracle DataDirect driver, then you must specify a connection property to the datasource.</p> <ul style="list-style-type: none"> <li>Use the following definitions for the Oracle DataDirect driver connection property:<br/><i>DataIntegrityLevel=required;EncryptionLevel=required;DataIntegrityTypes=(MD5,SHA1)</i></li> <li>If you use CRYPTO_CHECKSUM_TYPES in your sqlnet.ora, use the following examples: <ul style="list-style-type: none"> <li>oracle.net.encryption_client=rc4_256;oracle.net.crypto_checksum_types_client=MD5</li> <li>oracle.net.encryption_client=aes256;oracle.net.crypto_checksum_types_client=MD5</li> <li>oracle.net.encryption_client=rc4_256;oracle.net.crypto_checksum_types_client=SHA1</li> </ul> </li> <li>To authenticate to Oracle LDAP, which is also known as OID, use the LDAP server host or IP, the LDAP server port, the Oracle instance name and the realm. Enter the custom URL <i>jdbc:guardium:oracle:@ldap://w13ku2x32t4:389/on0maver;cn=OracleContext;dc=vguardium;dc=com</i></li> <li>The Oracle default user sys, is the owner of the database instance and has super user privileges, similar to root on Unix. The SYSDBA role has administrative privileges that are required to perform many high-level administrative operations such as starting and stopping the database, as well as performing operations such as backup and recovery. This SYSDBA role can also be granted to other users. The phrase sys as SYSDBA refers to the connection method required to connect as the sys user.</li> <li>To monitor values for Oracle 10 open source driver, enter the connection property: <i>internal_logon=sysdba</i></li> <li>To use the SYSDBA role, enter the connection property <i>SysLoginRole=sysdba</i></li> <li>To initiate an SSL datasource connection with server signed or mutual authentication, enter the connection property: <i>EncryptionMethod=SSL</i>.</li> </ul> <p>For an Oracle encrypted connection, define the connection property as:<br/><i>oracle.net.encryption_client=REQUIRED;oracle.net.encryption_types_client=RC4_40</i>. Note: A datasource that is defined to use 3DES168 encryption, throws an ORA-17401 protocol error or ORA-17002 checksum error when it encounters any SQL error. To fix this error, close and reopen the connection.</p> <p>If the connection is unsuccessful because the HostNameInCertificate does not match, enter this string as the connection property using the certificate name provided in the error message: <i>EncryptionMethod=SSL;HostNameInCertificate=certificate name</i>.</p> |
| Custom URL          | <p>The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.</p> <ul style="list-style-type: none"> <li>When you specify a Custom URL field with the Oracle Open Source format, specify <i>jdbc:guardium:oracle://:SID=&lt;SID&gt;</i>.</li> <li>When you create a datasource for an Oracle database with Oracle Advanced Security enabled, specify <i>EncryptionLevel=required</i> in the Custom URL field of the datasource definition.</li> </ul> <p>To initiate an SSL datasource connection using the Oracle JDBC driver, setup the connection URL using one of the examples below. Refer to the Oracle JDBC connection syntax.</p> <p>Example:</p> <pre>jdbc:oracle:thin:@(description= (address=(protocol=tcp)(port=1522)(host=adwc.uscom-west-1.oraclecloud.com))(connect_data=(service_name=VOVO0MKSEWWJ3PSJ_ISVDRIVERSDB_medium.dwcs.oracle.com))(security=(ssl_server_cert_dn="CN=adwc-dev.uscom-east-1.oraclecloud.com,OU=Testing Domain,O=End Point,L=Redwood Shores,ST=California,C=US"))</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Adding custom properties for classification

By default, the classifier uses `count *` to determine cardinality for random sampling. For Oracle datasources, Guardium supports alternative methods for determining cardinality: the DATA-CARDINALITY-FOR-SAMPLING-TABLES custom property for tables, and the DATA-CARDINALITY-FOR-SAMPLING-VIEWS-PERCENTAGE custom property for views.

### DATA-CARDINALITY-FOR-SAMPLING-TABLES

When sampling tables, this custom property uses database statistics to determine cardinality. To enable the database statistics method, add DATA-CARDINALITY-FOR-SAMPLING-TABLES = STATISTICS as a custom property for the datasource. When using this property, the classifier retrieves the number of rows from the `all_tables` data dictionary view.

Notes:

- The property name must be entered as DATA-CARDINALITY-FOR-SAMPLING-TABLES (all capital letters, with hyphens), and the only valid value is STATISTICS.
- The value of num\_rows in all\_tables might not be up-to-date. When using this property, work with your Oracle administrator to ensure the database statistics are current.

- After you run the discovery scenario with DATA-CARDINALITY-FOR-SAMPLING-TABLES = STATISTICS, click the  for the data source in the Process Run Log. You can see that the datasource is using the custom property.

#### DATA-CARDINALITY-FOR-SAMPLING-VIEWS-PERCENTAGE

When sampling views, this custom property provides a percentage value that the classifier uses to determine the sample. To enable this method, add DATA-CARDINALITY-FOR-SAMPLING-VIEWS-PERCENTAGE = [0.000001 to <100] as a custom property for the datasource. This method uses `sample_percent` where the specified value is the probability that each row is selected for the sample.

Note:

- The property name must be entered as DATA-CARDINALITY-FOR-SAMPLING-VIEWS-PERCENTAGE (all capital letters, with hyphens), and the allowed values are 0.000001 to <100.

You can add or change custom properties from either the Guardium UI or by using GRDAPi commands. After you add the custom properties, the information displays in the Details for datasource output. For more information about adding custom properties from the UI, see [Configuring custom properties for your datasources](#).

You can also use GRDAPi to manage custom properties. For example, assuming a datasource created with the following command:

```
grdapicreate_datasource type="Oracle (DataDirect - Service Name)" user="dbusername" password="yourdbpassword"
host="dbhostname" name="nameofthisdbconnection" shared=true application="Classifier" port=1521 serviceName="on9stuff"
dbName="nameofschema"
```

Use the following commands to create the DATA-CARDINALITY-FOR-SAMPLING-TABLES and DATA-CARDINALITY-FOR-SAMPLING-VIEWS-PERCENTAGE custom properties:

```
grdapicreate_datasource_custom_property name=DATA-CARDINALITY-FOR-SAMPLING-TABLES values=STATISTICS
grdapicreate_datasource_custom_property name=DATA-CARDINALITY-FOR-SAMPLING-VIEWS-PERCENTAGE values=10
```

Then use the following commands to add the properties to the Oracle datasource:

```
grdapicustom_property_to_datasource_by_name customProps="DATA-CARDINALITY-FOR-SAMPLING-TABLES=STATISTICS"
name="nameofthisdbconnection"
grdapicustom_property_to_datasource_by_name customProps="DATA-CARDINALITY-FOR-SAMPLING-VIEWS-PERCENTAGE=10"
name="nameofthisdbconnection"
```

For more information about the custom property APIs, see [Datasource custom property APIs](#).

## CAS (Configuration Auditing System) database instance

If you are a CAS user, configure the CAS database instance.

| Field     | Description                     |
|-----------|---------------------------------|
| Account   | The Oracle installation user.   |
| Directory | The directory of \$ORACLE_HOME. |

## Oracle (Data Direct - SID)

Configure an Oracle datasource with DataDirect connection on your Guardium® system.

### Supported Authentication Methods

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | Yes       |
| Kerberos       | No        |
| SSL            | Yes       |
| Mutual SSL     | Yes       |

## Parameters

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                                                                                                         |
| Port number         | Required. Default value: 1521.                                                                                                                                                                                                                                                                                                                                                  |
| SID name            | The Oracle system ID.                                                                                                                                                                                                                                                                                                                                                           |
| Schema              | The name of the database schema.                                                                                                                                                                                                                                                                                                                                                |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon. For examples, refer to the database vendor's JDBC documentation.                                                                                   |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.<br>Example:<br><code>jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCPS)(HOST=hostname.domain.com ip address )(PORT=1525)))(CONNECT_DATA=(SERVER=DEDICATED)(SID=Oracle_SID))</code> |

## Adding custom properties for classification

By default, the classifier uses `count *` to determine cardinality for random sampling. For Oracle datasources, Guardium supports alternative methods for determining cardinality: the DATA-CARDINALITY-FOR-SAMPLING-TABLES custom property for tables, and the DATA-CARDINALITY-FOR-SAMPLING-VIEWS-PERCENTAGE custom property for views.

#### DATA-CARDINALITY-FOR-SAMPLING-TABLES

When sampling tables, this custom property uses database statistics to determine cardinality. To enable the database statistics method, add DATA-CARDINALITY-FOR-SAMPLING-TABLES = STATISTICS as a custom property for the datasource. When using this property, the classifier retrieves the number of rows from the `all_tables` data dictionary view.

Notes:

- The property name must be entered as DATA-CARDINALITY-FOR-SAMPLING-TABLES (all capital letters, with hyphens), and the only valid value is STATISTICS.
- The value of num\_rows in all\_tables might not be up-to-date. When using this property, work with your Oracle administrator to ensure the database statistics are current.
- After you run the discovery scenario with DATA-CARDINALITY-FOR-SAMPLING-TABLES = STATISTICS, click the  for the data source in the Process Run Log. You can see that the datasource is using the custom property.

#### DATA-CARDINALITY-FOR-SAMPLING-VIEWS-PERCENTAGE

When sampling views, this custom property provides a percentage value that the classifier uses to determine the sample. To enable this method, add DATA-CARDINALITY-FOR-SAMPLING-VIEWS-PERCENTAGE = [0.000001 to <100] as a custom property for the datasource. This method uses `sample_percent` where the specified value is the probability that each row is selected for the sample.

Note:

- The property name must be entered as DATA-CARDINALITY-FOR-SAMPLING-VIEWS-PERCENTAGE (all capital letters, with hyphens), and the allowed values are 0.000001 to <100.

You can add or change custom properties from either the Guardium UI or by using GRDAPIS commands. After you add the custom properties, the information displays in the Details for datasource output. For more information about adding custom properties from the UI, see [Configuring custom properties for your datasources](#).

You can also use GRDAPIS to manage custom properties. For example, assuming a datasource created with the following command:

```
grdapi create_datasource type="Oracle (DataDirect - SID)" user="dbusername" password="yourdbpassword" host="dbhostname" name="nameofthisdbconnection" shared=true application="Classifier" port=1521 serviceName="on9stuff" dbName="nameofschema"
```

Use the following commands to create the DATA-CARDINALITY-FOR-SAMPLING-TABLES and DATA-CARDINALITY-FOR-SAMPLING-VIEWS-PERCENTAGE custom properties:

```
grdapi create_datasource_custom_property name=DATA-CARDINALITY-FOR-SAMPLING-TABLES values=STATISTICS
grdapi create_datasource_custom_property name=DATA-CARDINALITY-FOR-SAMPLING-VIEWS-PERCENTAGE values=10
```

Then use the following commands to add the properties to the Oracle datasource:

```
grdapi add_custom_property_to_datasource_by_name customProps="DATA-CARDINALITY-FOR-SAMPLING-TABLES=STATISTICS" name="nameofthisdbconnection"
grdapi add_custom_property_to_datasource_by_name customProps="DATA-CARDINALITY-FOR-SAMPLING-VIEWS-PERCENTAGE=10" name="nameofthisdbconnection"
```

You can also use GRDAPIS to update the custom properties:

```
grdapi update_datasource_custom_property name=DATA-CARDINALITY-FOR-SAMPLING-VIEWS-PERCENTAGE addValues=1,2,5
```

For more information about the custom property APIs, see [Datasource custom property APIs](#).

## CAS (Configuration Auditing System) database instance

If you are a CAS user, configure the CAS database instance.

| Field     | Description                     |
|-----------|---------------------------------|
| Account   | The Oracle installation user.   |
| Directory | The directory of \$ORACLE_HOME. |

## Percona MySQL

Configure a Percona MySQLdatasource on your Guardium® system.

Note: To use this feature, you must install the latest Guardium Vulnerability Assessment patch for version 11.5.

## Supported Authentication Methods

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | No        |
| Kerberos       | No        |
| SSL            | Yes       |
| Mutual SSL     | Yes       |

## Parameters

| Field               | Description                                                                                                                                                                                                                                                                                      |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                          |
| Port number         | Required. Default value: 3306.                                                                                                                                                                                                                                                                   |
| Database            | The name of the database.                                                                                                                                                                                                                                                                        |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                        |

## CAS (Configuration Auditing System) database instance

If you are a CAS user, configure the CAS database instance.

| Field     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account   | The name of the account owner.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Directory | The name of the installation directory.<br>Example for rpm and yum installation:<br><br><i>MYSQL_HOME=/var/lib/mysql/</i><br><br>Note:<br><i>MYSQL_HOME</i> is the environment variable containing the path to the directory holding the server-specific my.cnf file.<br><br>If <i>MYSQL_HOME</i> is not set, and the server is started with mysqld_safe, <i>MYSQL_HOME</i> is set as follows: If there is a <i>my.cnf</i> file in the MySQL data directory, but not in the MySQL base directory, <i>MYSQL_HOME</i> is set to the MySQL data directory. Else, <i>MYSQL_HOME</i> is set to the MySQL base directory. |

## PostgreSQL

Configure a PostgreSQL datasource on your Guardium® system.

## Supported Authentication Methods

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | No        |
| Kerberos       | No        |
| SSL            | Yes       |
| Mutual SSL     | Yes       |

## Parameters

| Field               | Description                                                                                                                                                                                                                                                                                      |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                          |
| Port number         | Required. Default value: 5432.                                                                                                                                                                                                                                                                   |
| Database            | Required. The name of the database.<br>For example, <i>postgres</i> .<br>For Vulnerability Assessment (VA) tests that require scanning other databases, the VA assessment scan will get a list of all required databases from the PostgreSQL instance and run the test.                          |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                        |

## Adding custom property for classification

12.1 and later To improve the performance of Guardium classification scans, you can add the following custom property for PostgreSQL.

- LARGE-TEXT-DATA-TYPE-MAX-LENGTH - By default, when scanning large data types like XML, VARCHAR(MAX), or TEXT, the classifier samples only the first 3000 characters. Use the LARGE-TEXT-DATA-TYPE-MAX-LENGTH property to define a custom length in the range of 0 - 2147483647 characters.

You can add or change custom properties from either the Guardium UI or by using GRD API commands. After you add the custom properties, the information is displayed in the Details for datasource output. For more information about adding custom properties from the UI, see [Configuring custom properties for your datasources](#).

For more information about classification, see [Discover Sensitive Data](#).

## SAP HANA

Configure a SAP HANA datasource on your Guardium® system.

## Supported Authentication Methods

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | No        |
| Kerberos       | No        |
| SSL            | Yes       |
| Mutual SSL     | No        |

## Parameters

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Port number         | Required. Default value: 30015.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Database            | Required. The name of the database.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation.<br>Configuring SSL:<br><br>When you create your server's public and private key pair or public key certificate, the Common Name (CN) must match the server's hostname and use the Fully Qualified Domain Name (FQDN). The Subject Alternative Name (SAN) must use the server's hostname with FQDN and the server's IP.<br><br>If SSL is incorrectly configured, the connection fails because the hostname cannot be verified. To bypass a hostname verification error, use the following workaround:<br><br>Set the connection property <i>hostNameInCertificate=ServerHostname</i> . Where <i>ServerHostname</i> is the CN that was used in the certificate and not the hostname with which the connection was established. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## CAS (Configuration Auditing System) database instance

If you are a CAS user, configure the CAS database instance.

| Field     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account   | Required. The name of the account owner.<br>The syntax is <SID>adm<br><br>Example: <i>hxeadm</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Directory | Required. The name of the installation directory.<br>You can specify multiple paths for the database instance directory. Indicate a separate path by using a pipe " " with spaces.<br><br>For example:<br><br><i>/usr/sap/HXE/home   SID=HXE   logpath=/hana/shared/log   datapath=/hana/shared/data   installpath=/usr/sap .</i><br><br>Where: <ul style="list-style-type: none"><li>• /usr/sap/HXE/home is the home directory for the instance account.</li><li>• SID=HXE is the system ID. The SAP system ID (SID) is the identifier for the SAP HANA system.</li><li>• logpath=/hana/shared/log is the path to the log directory of the SAP HANA system. The default log location is /hana/log/&lt;SID&gt;.</li><li>• datapath=/hana/shared/data is the path to the data directory of the SAP HANA system. The default data location is /hana/data/&lt;SID&gt;.</li><li>• installpath=/usr/sap is the installation path that is specific to the operating system on which the SAP HANA studio is installed. As an example, for Linux, the installation path is /usr/sap for Linux.</li></ul><br>All the paths that are listed in this example are required entries. |

## Snowflake

Configure a Snowflake datasource on your Guardium® system.

## Supported Authentication Methods

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | No        |
| Kerberos       | No        |
| SSL            | Yes       |
| Mutual SSL     | No        |

Note:

The default authentication method is SSL.

## Parameters

| Field               | Description                                                                                                                                                                                                                                                                                      |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname of the datasource.                                                                                                                                                                                                                                                        |
| Port number         | Required. Default value: 443                                                                                                                                                                                                                                                                     |
| Database            | The name of the database.                                                                                                                                                                                                                                                                        |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation. |

## SQL DB Azure

Configure an SQL DB Azure datasource on your Guardium® system.

## Supported Authentication Methods

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | No        |
| Kerberos       | No        |
| SSL            | No        |
| Mutual SSL     | No        |

## Parameters

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                                                                                                     |
| Port number         | Required. Default value: 1433                                                                                                                                                                                                                                                                                                                                               |
| Database            | The name of the database.<br>For security assessments, the required value is master.                                                                                                                                                                                                                                                                                        |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the Microsoft SQL Server JDBC driver documentation.<br>Note: Azure Active Directory authentication is not supported. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                                                                                                   |

## Sybase

Configure a Sybase datasource on your Guardium® system.

## Supported Authentication Methods

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | No        |
| Kerberos       | No        |
| SSL            | Yes       |
| Mutual SSL     | No        |

## Parameters

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                                                                                                      |
| Port number         | Required. Default value: 4100.                                                                                                                                                                                                                                                                                                                                               |
| Database            | The name of the database. For Vulnerability Assessment, use the database instance name.                                                                                                                                                                                                                                                                                      |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation.<br>For a default character set of Roman 8, enter the property charSet=utf8. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                                                                                                    |

## CAS (Configuration Auditing System) database instance

---

If you are a CAS user, configure the CAS database instance.

| Field     | Description                                                                                                                                                                                              |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account   | The name of the account owner. Often <code>sybase</code> .                                                                                                                                               |
| Directory | The name of the installation directory.<br>For UNIX, enter <code>/home/sybase</code><br><br>For Windows, enter <code>C:\sybase</code><br><br>An environment variable <code>SYBASE</code> may be defined. |

## Adding custom property for classification

---

12.1 and later To improve the performance of Guardium classification scans, you can add the following custom property for Sybase.

- `LARGE-TEXT-DATA-TYPE-MAX-LENGTH` - By default, when scanning large data types like XML, `VARCHAR(MAX)`, or `TEXT`, the classifier samples only the first 3000 characters. Use the `LARGE-TEXT-DATA-TYPE-MAX-LENGTH` property to define a custom length in the range of 0 - 2147483647 characters.

You can add or change custom properties from either the Guardium UI or by using GRD API commands. After you add the custom properties, the information is displayed in the Details for datasource output. For more information about adding custom properties from the UI, see [Configuring custom properties for your datasources](#).

For more information about classification, see [Discover Sensitive Data](#).

## Sybase IQ

---

Configure a Sybase IQ datasource on your Guardium® system.

## Supported Authentication Methods

---

| Authentication | Supported                                                                                                                                         |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Local user     | Yes                                                                                                                                               |
| LDAP           | No                                                                                                                                                |
| Kerberos       | No                                                                                                                                                |
| SSL            | Yes. Limited support for encrypted TDS connections over TLS in some versions only. For more information, see the database vendor's documentation. |
| Mutual SSL     | No                                                                                                                                                |

## Parameters

---

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                                                                                                                                                                                             |
| Port number         | Required. Default value: 2638.                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Database            | The name of the database.                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is <code>property1=value;property2=value</code> , where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation.<br>To use SSL, set <code>ENCRYPT_PASSWORD=true</code> .<br>Note: You must start the Sybase IQ server with the parameter <code>TDS=ENCRYPTED</code> . |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                                                                                                                                                                                           |

## TERADATA

---

Configure a TERADATA datasource on your Guardium® system.

## Supported Authentication Methods

---

| Authentication | Supported |
|----------------|-----------|
| Local user     | Yes       |
| LDAP           | No        |
| Kerberos       | No        |
| SSL            | No        |
| Mutual SSL     | No        |

## Parameters

---

| Field | Description |
|-------|-------------|
|       |             |

| Field               | Description                                                                                                                                                                                                                                                                                      |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name/IP        | Required. The hostname or IP address of the datasource.                                                                                                                                                                                                                                          |
| Port number         | Required. Default value: 1025.                                                                                                                                                                                                                                                                   |
| Database            | The name of the database.                                                                                                                                                                                                                                                                        |
| Connection property | Properties that must be included in the JDBC URL to establish a JDBC connection with the datasource. The required format is property1=value;property2=value, where each property and value pair is separated by a semicolon.<br>For examples, refer to the database vendor's JDBC documentation. |
| Custom URL          | The connection string to the datasource. When the custom URL is not provided, the datasource connection is made by using properties such as the hostname and port number.                                                                                                                        |

## Text datasources

Parameters to configure a text datasource.

### Parameters

| Text datasource | Port number |
|-----------------|-------------|
| Text            | 0           |
| Text:HTTP       | 8000        |
| Text:FTP        | 22          |
| Text:SAMBA      | 445         |
| Text:HTTPS      | 8443        |
| N_A             | 0           |

## Configuring custom properties for your datasources

Enrich your datasources by defining and assigning custom properties.

### About this task

By configuring custom properties, you can better manage your datasources, organize your workflow, and efficiently accomplish complex processes.

Consider a scenario where you'd like to assess the vulnerability of the datasources that are residing in a specific geographical location. You can define the name of the location as a custom property, assign the property to all the datasources that reside in that location, and group the datasources by the custom property. The custom property can also be added to an existing datasource group. You can now configure a security assessment to scan only the active datasources that are in the group.

Custom properties are flexible and can be reconfigured or deleted, as needed. You can create any number of customized properties based on your business needs and assign multiple properties to one datasource. You can also import existing values from the Guardium® compliance monitoring application. Manually import selected properties or dynamically import updated values when new properties are added to compliance monitoring. When you export your datasource, the assigned properties are also exported.

You can enrich your datasource in two simple steps:

1. Define a custom property with one or more associated values.
2. Assign the customized property to your datasource.

The following procedure describes the configuration process in detail.

### Procedure

1. Open the Datasource Definitions tool by clicking [Setup > Tools and Views > Datasource Definitions](#).
2. To add a new custom property, click [Custom properties > Manage](#)
  - a. From the Manage custom properties window, click  to create a custom property. In the Property name field, enter the name of the custom property. Example: Data center.
  - b. Under Valid values, click  to add one or more custom values to the custom property. Example: New York, San Francisco, Chicago.
  - c. Click Save.
  - d. Repeat steps [2.a](#) to [2.c](#) to add more custom properties based on your business needs. Examples: Country, Continent, Business unit. You can create any number of custom properties with any number of associated values.
3. To assign the custom property, select your datasource or datasource group from the Datasource Definitions page. Then click [Custom properties > Add to datasources](#).
  - a. Select the appropriate Property name from drop-down menu.
  - b. Select the appropriate Value from the drop-down menu.
  - c. Click  another to add another custom defined property to the datasource. You can add multiple properties to one datasource or datasource group.
  - d. Click Save to assign the properties to the selected datasource or group.
4. Optional: Assign additional properties by repeating step [3](#). You can also edit the datasource by selecting the datasource, then clicking , accessing the Custom tab, and selecting a different value for the datasource.
5. Optional: If applicable, import custom properties from industry and application groups that you have defined in your Guardium compliance monitoring application. You can import all or selected properties. Check Update custom datasource properties with industries and application updates to dynamically import properties and as when they are updated.

6. Optional: Edit or delete custom properties, as needed. When a custom property is deleted, it's also removed from all associated datasources and datasource groups.
7. View all the assigned properties for a datasource in the Datasource Definitions page under the Custom column.

## Related reference

---

- [Add custom properties to a datasource by ID](#)
- [Add custom properties to a datasource by name](#)
- [Add custom properties to datasources in a group](#)
- [Update the custom property in a datasource](#)
- [Delete the custom property in a datasource](#)
- [Remove the custom property from a datasource using the datasource ID](#)
- [Remove the custom property from a datasource using the datasource name](#)
- [Remove the custom property from datasources in a group](#)

---

## Working with existing datasources

After you create a datasource definition, you can clone, modify, or delete the datasource.

### Procedure

---

- To open the Datasource Definitions page, browse to Setup > Tools and Views > Datasource Definitions.
- From Datasource Definitions, you can use the horizontal scroll bar to see the application type for each datasource. Select a datasource of the application type that you want to modify.

## Cloning a datasource

---

### Procedure

- Select the datasource that you want to clone from the Select datasource window, and click .
- The cloned datasource displays Datasource Definition as **Copy of <original datasource>**. All of the information from the original datasource definition appears in the dialog. Change any of the fields as needed.
- Click Save to save the cloned datasource.

## Modifying a datasource

---

### Procedure

- Select the datasource that you want to modify from the Select datasource window, and click .
- The information that you entered when the datasource definition was created appears in the Datasource Definition dialog. Change any of the fields as needed.
- Click Save to save the changes that you made to the datasource.

## Deleting a datasource

---

### Procedure

From the Datasource Definitions page, select the datasource that you want to remove, and click . The datasource and all its references are deleted.

---

## Reporting on datasources

Guardium® provides reports on the datasources that are in your environment and any changes made to them.

### Procedure

---

- Open the Datasources report by navigating to Reports > Report Configuration Tools > Datasources. The table that appears lists all datasources, and the information that is stored in each datasource definition.
- Right-click any cell in the table and you are given two options: Datasource Version History, and Invoke.
  - Click Datasource Version History to view changes made to the datasource definition.
  - Click Invoke to select and run one of the available APIs for the datasource.

Note: You can customize the run time and presentation parameters of the Datasources report by clicking the pencil icon.

## Related concepts

---

- [Datasource APIs](#)

---

## Defining a datasource using a service name

You can define a datasource that enables your users to connect to an Oracle database by using the service name by using a custom URL.

## About this task

---

You must enter the hostname, port, service name, and the custom URL.

## Procedure

---

1. Determine the Oracle service name.

You can use commands like these:

```
SQL> set line size 5000;
SQL> select host_name, instance_name from v$instance;
SQL> select name from v$database;
SQL> show parameter service
```

Use the name that appears in the VALUE column.

2. Load the appropriate Oracle JDBC thin driver to the Guardium® system.

- a. Download the driver for your Oracle database from the Oracle website.
  - b. Open the Customer Uploads window by browsing to Harden > Vulnerability Assessment > Customer Uploads.
  - c. Locate the section titled Upload Oracle JDBC driver. Click Browse and browse to the location to which you downloaded the file. Click Use open-source driver for all.
  - d. Restart the Guardium user interface after the upload is complete.
3. Define the datasource for this database.
- a. Browse to Setup > Tools and Views > Datasource Definitions.
  - b. Select  to add an Oracle datasource.
  - c. Define the datasource as described in [Creating a datasource definition](#).
  - d. Enter the service name in the Service Name field. In the custom URL field, enter `jdbc:oracle:thin@//hostname:port/svcname` where `hostname` and `port` are the standard values for the database and `svcname` is same value that you entered in the Service Name field.
  - e. Click Save to save your changes.

## Managing KDC definitions

---

If your datasource requires authentication using Kerberos, you can specify the information needed for Guardium to obtain a Kerberos ticket before making the connection.

## About this task

---

You can assign a KDC to a specific datasource or managed unit group, to provide Guardium authentication for Mongo and Hive databases. The appliance gets a ticket via the JDBC connection, so the users do not need to get tickets themselves. Note that this is independent from what the appliance itself is set up to use.

You can define up to 5 Kerberos Key Distribution Centers (KDC) on a Central Manager, and one on a standalone Guardium. To add a Key Distribution Center to Guardium you specify:

- realm: domain name in uppercase letters
- KDC: hostname of the Kerberos server
- encryption type for Kerberos tickets
  - des-cbc-md5
  - des-cbc-crc
  - rc4-hmac
  - des3-cbc-sha1
  - aes128-cts-hmac-sha1-96
  - aes256-cts-hmac-sha1-96

The default is aes256-cts-hmac-sha1-96, which is the most secure encryption type.

## Procedure

---

1. Click Setup > Tools and Views > Kerberos configuration
2. Click  to create a new configuration.
3. Specify Name, KDC, and Realm.
4. Specify Encryption Type. The default is aes256-cts-hmac-sha1-96.
5. Click Save.

## What to do next

---

After you have created a Kerberos KDC, you can select it when configuring your datasource setup.

## Managing datasource credentials with CyberArk

---

Guardium supports the CyberArk Application Password Provider, a robust solution to the numerous maintenance and security challenges that arise in managing passwords. Use CyberArk to securely store, provision, audit, and manage your Guardium datasource credentials.

## Existing Challenges

---

- Datasource credentials are updated by database administrators, and manually passed on to users. Easy access to this highly sensitive information creates significant security risks and vulnerability.
- Periodical updates to passwords require manual synchronization across all datasources.
- The challenge is compounded in a large-scale environment where hundreds or thousands of datasource credentials require systematic maintenance.

## Benefits of using CyberArk with Guardium

---

- Credentials are defined, secured, and managed in a digital vault, eliminating the need to embed them locally in the Guardium system.
- Depending on business needs, any number of vaults can be configured by using the CyberArk web console.
- Passwords are automatically generated and replaced for all supported database types, meeting audit and regulatory requirements.
- The CyberArk Application Password Provider that is integrated with Guardium, allows retrieved credentials to be securely cached locally. This reduces the frequency in communication between the Guardium system and the CyberArk vault, improving speed and performance. If there is a network outage, the datasources remain intact and functional.
- **[CyberArk deployment overview](#)**  
The datasource credentials, along with access control, dependencies, and work flows are defined in the vault. Each Guardium system is then configured to access the vault, and retrieve the stored credentials. After the systems are set up, the passwords can be provisioned and maintained with no manual intervention.
- **[Setting up the CyberArk vault system](#)**  
The CyberArk administrator must set up and configure the CyberArk vault server. For detailed information, see the CyberArk documentation.
- **[Deploying CyberArk on your Guardium system](#)**  
The Guardium system administrator must use the following workflow to deploy CyberArk in the Guardium environment.
- **[Upgrading the CyberArk SDK on a central manager or standalone system](#)**  
When an upgrade patch is available, use this procedure to upgrade the CyberArk SDK on your central manager or standalone system .
- **[Upgrading the CyberArk SDK on a managed unit](#)**  
Use the GUI on the central manager to distribute the CyberArk upgrade credentials and upgrade patch to the managed units.
- **[Uninstalling CyberArk](#)**  
Uninstall CyberArk from your Guardium system using the Command line Interface.

## CyberArk deployment overview

---

The datasource credentials, along with access control, dependencies, and work flows are defined in the vault. Each Guardium® system is then configured to access the vault, and retrieve the stored credentials. After the systems are set up, the passwords can be provisioned and maintained with no manual intervention.

Here is an overview of the work flow that is used to deploy CyberArk:

1. Set up the vault system on CyberArk. For more information, see [Setting up the CyberArk vault system](#).
2. Download and install the CyberArk SDK patch. For more information, see [Downloading and installing the CyberArk SDK patch](#).
3. Install CyberArk on your Guardium system. For more information, see [Installing CyberArk](#).
4. Configure CyberArk. For more information, see [Configuring CyberArk on your Guardium system](#).
5. Define datasources by using CyberArk credentials. For more information, see [Defining Guardium datasources to access CyberArk](#).

## Setting up the CyberArk vault system

---

The CyberArk administrator must set up and configure the CyberArk vault server. For detailed information, see the CyberArk documentation.

Use this workflow to set up the CyberArk vault system.

1. Verify that your databases are supported by CyberArk for automatic password provisioning. If your database is not supported, you can continue to store your credentials on CyberArk. However, the passwords are not automatically provisioned.
  2. Set up a vault in the CyberArk vault server.
  3. Set up one or multiple safes within the CyberArk vault.
  4. Populate the safe with the CyberArk objectnames (Guardium® datasource names) and their respective passwords.
  5. Create a group and make it the owner of the safe. All safes inherit the group's permissions automatically.
  6. Create a CyberArk application ID by using the CyberArk web console and grant the necessary permissions. For more information, see [Creating an application ID on CyberArk](#). This application ID is used to configure CyberArk on your Guardium system.
  7. Provide the following information to the Guardium system administrator:
    - Vault host name or IP address
    - Vault user name
    - Vault password
    - Standby vault server IP address list, if any
    - Group name, Application IDs, corresponding safe names, and folder names
    - CyberArk objectnames
- **[Creating an application ID on CyberArk](#)**  
The CyberArk administrator must create an application ID, assign it to a safe, and grant the required permissions. This application ID is used to configure the Guardium system.
  - **[Adding and removing account permissions on CyberArk](#)**  
The CyberArk administrator can grant or revoke permissions to the Guardium system on the CyberArk vault server.

## Creating an application ID on CyberArk

---

The CyberArk administrator must create an application ID, assign it to a safe, and grant the required permissions. This application ID is used to configure the Guardium system.

## Before you begin

---

The safe that you use to store your CyberArk objectnames (Guardium datasources) must be set up in the CyberArk vault.

## Procedure

---

1. Log in to the CyberArk web console.
2. Select Applications from the menu bar and click Add Application.
3. In the name field, enter an arbitrary Application ID name. All the other fields can remain empty. Click Add to add the application.
4. In the menu bar, select Policies > Access Control (Safes) and click the safe that you use to store your CyberArk objectnames.
5. Click Members to view the safe details.
6. On the Members tab, click Add Member to access the Add Safe Member screen.
7. In the Search field, enter your Application ID name, and click Search.
8. Select your application ID name from the search results. Mark the check box for Retrieve Accounts, and clear the check boxes for all other enabled permissions.
9. Click Add to add the application ID to the safe.

## What to do next

---

If you are using multiple safes to store CyberArk objectnames, repeat steps 2 - 9 to create and assign application IDs for each safe.

Provide the application ID, corresponding safe name, and folder name to your Guardium system administrator. Each Guardium datasource is configured to access the safe that is assigned to this application ID.

## Adding and removing account permissions on CyberArk

---

The CyberArk administrator can grant or revoke permissions to the Guardium system on the CyberArk vault server.

The Guardium system's account inherits all permissions from the group that it is added to. The minimum group permissions that are required are: List, Retrieve, and View Accounts.

Use the following procedures to add or remove the Guardium system's account from the CyberArk group.

## Providing permission to the Guardium system

---

Use the following procedure to provide permission to the Guardium system on CyberArk.

Note: The CyberArk administrator must grant permission to complete installation of CyberArk on the Guardium system.

1. Use the CyberArk client to log in to vault server.
2. From the menu, go to Tools > Administrative Tools > Users and Groups.
3. On the Users and Groups on Server Vault page, select the group that owns your safe. Click Update.
4. On the Update group page, click Add and select User from the drop-down menu.
5. On the Add Members to Group page click the Applications folder, select the member (Guardium system's account name) *Prov\_Guardium system's address*, and click the right arrow button to move the member to the group.
6. Click ok to add the account to the group.

## Revoking the Guardium system's permissions on CyberArk

---

When CyberArk is uninstalled from the Guardium system, use the following procedure to revoke permissions on CyberArk.

Note: To reinstall CyberArk on your Guardium system, you must remove the CyberArk account from the group.

1. Use the CyberArk client to log in to vault server.
2. From the menu, go to Tools > Administrative Tools > Users and Groups.
3. On the Users and Groups on Server Vault page, click the Applications folder, and select the member (Guardium system's account name) *Prov\_Guardium system's address*.
4. Click Delete to remove the account from the group.

## Deploying CyberArk on your Guardium system

---

The Guardium system administrator must use the following workflow to deploy CyberArk in the Guardium environment.

1. [Downloading and installing the CyberArk SDK patch](#)  
Download and install the CyberArk SDK patch on your Guardium® system.
2. [Installing CyberArk](#)  
Install CyberArk on your Guardium system by using the Command Line Interface.
3. [Configuring CyberArk on your Guardium system](#)  
Create a CyberArk application ID configuration on your Guardium system to access the assigned CyberArk safe.
4. [Defining Guardium datasources to access CyberArk](#)  
Configure the datasources on your Guardium system for automatic password provisioning. You can create a new datasource definition or edit an existing definition.

# Downloading and installing the CyberArk SDK patch

Download and install the CyberArk SDK patch on your Guardium® system.

## Before you begin

The CyberArk SDK/module/installer that is used by IBM Guardium is under restriction by CyberArk from export to certain areas of the world. To obtain this software, you must contact IBM support by [opening an IBM support case](#) to ensure compliance with these restrictions before downloading. In the case description, mention the geographic location, specifically the Country and State, of your Guardium deployment where the CyberArk patch will be deployed.

## Procedure

1. Download the CyberArk SDK patch to your central manager or standalone system.
2. Install the patch by using the command **store system patch install sys** and entering the patch number to install. To install the patch on a managed unit, use the GUI of the central manager to distribute the patch to one or more managed units. For more information, see [Central Patch Management](#).

Next topic: [Installing CyberArk](#)

# Installing CyberArk

Install CyberArk on your Guardium system by using the Command Line Interface.

## Before you begin

- The CyberArk administrator must set up the vault system with the required permissions.
- Obtain the CyberArk vault hostname or IP address, vault username, and vault password from the CyberArk administrator.
- If you installed CyberArk before, your Guardium system's account, *Prov\_Guardium system's address*, can exist in the CyberArk vault server. Delete the account from the vault server before you begin installation. For more information, see [Revoking the Guardium system's permissions on CyberArk](#).

## Procedure

1. Using the Guardium CLI, run the command **store cyberark install**.
2. If you meet the prerequisites, type **yes**.
3. When prompted, enter the vault hostname or IP address, the vault username, and vault password.
4. If you have standby vault servers available, you can optionally configure them now.  
A standby vault server IP list is a group of vault IP addresses that are set up by the CyberArk administrator. These vaults are used as a backup when a connection cannot be made to the primary vault server.
  - a. To add the standby vault server IP address list to your Guardium system, run the CLI command **store cyberark config\_failover**.
  - b. Enter a comma-separated list of CyberArk vault server IP addresses beginning with your primary vault server's IP address. The CyberArk Application Password Provider connects to the first available IP address on the list. If a connection cannot be made, the agent tries to access the next available IP address until it can successfully connect to a CyberArk vault server.
  - c. Confirm the new IP address list.

## What to do next

Provide the Guardium system's account name that is generated during the installation, to the CyberArk administrator. This account must be granted the appropriate permissions on the CyberArk vault server. For more information, see [Providing permission to the Guardium system](#).

After the account is granted permission, configure the CyberArk application ID on your Guardium system. For more information, see [Configuring CyberArk on your Guardium system](#).

Previous topic: [Downloading and installing the CyberArk SDK patch](#)

Next topic: [Configuring CyberArk on your Guardium system](#)

# Configuring CyberArk on your Guardium system

Create a CyberArk application ID configuration on your Guardium system to access the assigned CyberArk safe.

## Before you begin

Obtain the application IDs, corresponding safe names, and folder names from your CyberArk administrator.

## About this task

Each CyberArk application ID must be configured on your Guardium system to access the assigned CyberArk safe.

## Procedure

1. Log in to your Guardium system as the `admin` user.
2. Go to `Setup > Tools and Views > CyberArk Configurations`.
3. Click  to open the Create New CyberArk Configuration dialog.
4. In the `Name` box, enter an arbitrary name for the configuration. This name is used to configure your Guardium datasources to access the CyberArk vault.
5. In the `Application ID` box, enter the name of your application ID provided by your CyberArk administrator.
6. In the `Safe Name` box, enter the name of the CyberArk safe that is assigned to the Application ID.
7. In the `Folder Name` box, enter the name of the folder where the CyberArk safe is located.
8. Click `Save` to save the configuration.
9. If you have multiple application IDs, you can optionally create multiple configurations on your Guardium system by repeating steps 3 to 8. Alternatively, use the Guardium API command `create_cyberark_config`. For more information, see [create\\_cyberark\\_config](#).

## What to do next

Set up your Guardium datasources to access the credentials stored on CyberArk. For more information, see [Defining Guardium datasources to access CyberArk](#).

Previous topic: [Installing CyberArk](#)

Next topic: [Defining Guardium datasources to access CyberArk](#)

## Defining Guardium datasources to access CyberArk

Configure the datasources on your Guardium® system for automatic password provisioning. You can create a new datasource definition or edit an existing definition.

### Before you begin

Obtain the CyberArk objectname from your CyberArk administrator for each corresponding Guardium datasource.

### Procedure

1. To access an existing datasource definition, go to `Setup > Tools and Views > Datasource Definitions`, and click . To create a new datasource definition, see [Creating a datasource definition](#).
2. Configure the Credential type by selecting the External password radio button.
3. In the External password type Location drop-down, select CYBERARK.
4. In the CyberArk config drop-down, select the name of the CyberArk configuration that contains the Guardium datasource credential. For more information, see [Configuring CyberArk on your Guardium system](#).
5. In the CyberArk object name Location box, enter CyberArk objectname that corresponds with the Guardium datasource credential.
6. Click `Save`.
7. Click `Test connection` to ensure that the Guardium system can connect to the CyberArk vault and fetch the datasource credential.

## What to do next

Repeat steps 2 to 7 to configure all your Guardium datasources to access CyberArk.

Note: To provision passwords with no manual intervention, ensure that the CyberArk administrator enabled automatic management for your Guardium system's account. If your database is not supported, you can continue to store your credentials on CyberArk. However, the passwords are not automatically provisioned.

Previous topic: [Configuring CyberArk on your Guardium system](#)

## Upgrading the CyberArk SDK on a central manager or standalone system

When an upgrade patch is available, use this procedure to upgrade the CyberArk SDK on your central manager or standalone system .

### Before you begin

- Download the CyberArk upgrade patch.
- Obtain the CyberArk credentials that are required to connect to the CyberArk vault from the CyberArk administrator. The credentials that are required are the CyberArk vault web server hostname or IP address, the vault username, and the vault password.

### Procedure

1. Using the Guardium® CLI, enter the CyberArk credentials by using the command `store cyberark upgrade_parameter`.
2. Run the command `show system patch available` to list the patches that are available.
3. Run the CLI command `store system patch install sys` and enter the patch number to install.
4. Run the CLI command `show system patch installed` to display the status of the upgrade patch. If required, rerun the command to view the updated status of the installation.

## Upgrading the CyberArk SDK on a managed unit

Use the GUI on the central manager to distribute the CyberArk upgrade credentials and upgrade patch to the managed units.

## Before you begin

---

- Download the CyberArk upgrade patch.
- Obtain the CyberArk upgrade credentials that are required to connect to the CyberArk vault from the CyberArk administrator. The credentials that are required are the CyberArk vault web server hostname or IP address, the vault username, and the vault password.

## Procedure

---

1. On the central manager's GUI, access Manage > Central Management > Distribute Configuration Profiles.
  2. Create a CyberArk configuration profile, enter the CyberArk upgrade credentials, and distribute the profile to the managed units. For more information, see [Working with configuration profiles](#).
  3. Distribute the upgrade patch to the managed units. For more information on patch distribution, see [Central Patch Management](#).
- 

## Uninstalling CyberArk

Uninstall CyberArk from your Guardium system using the Command line Interface.

## Before you begin

---

To uninstall the CyberArk Application Password Provider, you must remove the corresponding entry for your Guardium system from the CyberArk vault server first. For more information, see [Revoking the Guardium system's permissions on CyberArk](#).

## Procedure

---

1. Using the Guardium CLI, run the command **store cyberark uninstall**.
  2. Type **yes** in the Guardium CLI to uninstall CyberArk.
- 

## Managing datasource credentials with AWS Secrets Manager

Integrate your Guardium® system with the Amazon Web Services (AWS) Secrets Manager to securely store, manage, rotate, and retrieve credentials for your datasources that use the Amazon Relational Database Service (RDS).

1. [Gathering required information from AWS Secrets Manager](#)  
Obtain the AWS Secrets Manager configuration information from the AWS management console.
  2. [Creating a secret user](#)  
Create a database user and assign credentials.
  3. [Creating a secret key](#)  
Create and configure a secret name and secret access key for the secret user on the AWS management console.
  4. [Selecting the authentication type and setting up roles](#)  
Guardium supports three authentication types to connect to the AWS Secrets Manager and AWS database services - Security Credentials, IAM Role, and IAM Instance Profile. Set up and configure the authentication type for your Guardium datasource.
  5. [Configuring the AWS Secrets Manager on your Guardium system](#)  
Configure the AWS Secrets Manager on your Guardium system. Each secret user must be configured on your Guardium system to access the AWS Secrets Manager.
  6. [Defining Guardium datasources to access AWS Secret Manager](#)  
Configure the datasources on your Guardium system for automatic password provisioning using the AWS Secrets Manager. You can create a new datasource definition or edit an existing definition.
- 

## Gathering required information from AWS Secrets Manager

Obtain the AWS Secrets Manager configuration information from the AWS management console.

## Before you begin

---

Ensure that the RDS service for your datasources is created.

## Procedure

---

Login to the AWS management console as an administrator and gather the following information:

- DB identifier (Guardium® instance name)
- DB name (Guardium service name)
- Endpoint (Guardium host name)
- Port number
- The location of your AWS data center.

Next topic: [Creating a secret user](#)

## Creating a secret user

Create a database user and assign credentials.

### Procedure

Your database administrator must create a database user (secret user) for your Guardium® datasource. The username and password that are assigned to this user are managed by the AWS Secrets Manager.

### What to do next

Note the username and password. This information is used when you create a secret key.

Previous topic: [Gathering required information from AWS Secrets Manager](#)

Next topic: [Creating a secret key](#)

## Creating a secret key

Create and configure a secret name and secret access key for the secret user on the AWS management console.

### Before you begin

Ensure that you have the secret username and password that you used to create a secret user. For more information, see [Creating a secret user](#).

### Procedure

1. Log in to the Amazon AWS management console and ensure that you are connected to the relevant data center.
2. Access Services > Security, Identity, & Compliance > Secrets Manager to view, edit, or create a secret.
3. Edit a secret by clicking the Secret name. To create a secret, click Store a new secret.
4. Select the secret type by clicking Credentials for RDS database.
5. Enter the secret username and password.
6. Use the DefaultEncryptionKey to encrypt your secret information.
7. Choose your RDS database and click Next.
8. Enter a Secret name and description. This secret name is used in the Guardium® datasource definition to reference your datasource and retrieve the datasource credentials.
9. Select Enable automatic rotation and select the required rotation interval from the drop-down.
10. Select Create a new Lambda function to perform rotation.
11. In the SecretsManager field, enter your secret name.
12. Under Select which secret will be used to perform the rotation select Use this secret. Then, click Next.
13. Review your entries, then click Store.

## Results

You can now click the Secret name to do the following:

- View the username and password by clicking Retrieve secret value.
- Change the password for the secret user, if required, by clicking Rotate secret immediately.

### What to do next

Note the name of the secret. This information is used when you define your datasources to retrieve credentials from the AWS Secrets Manager.

Previous topic: [Creating a secret user](#)

Next topic: [Selecting the authentication type and setting up roles](#)

## Selecting the authentication type and setting up roles

Guardium® supports three authentication types to connect to the AWS Secrets Manager and AWS database services - Security Credentials, IAM Role, and IAM Instance Profile. Set up and configure the authentication type for your Guardium datasource.

- [Authenticating by using security credentials](#)  
Create an access key ID and a secret access key to use this legacy authentication type.
- [Authenticating by using IAM Role](#)  
The IAM role authentication type allows for an IAM Instance Profile to be assumed by specifying a Role Amazon Resource Name (ARN) in addition to an access key ID and secret access key. In this authentication scenario, temporary security credentials are used to connect to AWS Secrets Manager/AWS Secret Manager or AWS database services.
- [Authenticating by using IAM instance profile](#)  
You can authenticate by using the IAM instance profile only when you use a Guardium instance that is deployed on AWS EC2.

Previous topic: [Creating a secret key](#)

Next topic: [Configuring the AWS Secrets Manager on your Guardium system](#)

# Authenticating by using security credentials

Create an access key ID and a secret access key to use this legacy authentication type.

## Procedure

1. In the Amazon AWS management console, click your user name. From the menu, select My Security Credentials.
2. Under Access keys for CLI, SDK, & API access, select Create access key to generate an access key ID and secret access key.  
Note: If an access key ID and a secret access key already exist, you can delete them or make them inactive. However, you might lose connectivity to an application that is using the keys.

# Authenticating by using IAM Role

The IAM role authentication type allows for an IAM Instance Profile to be assumed by specifying a Role Amazon Resource Name (ARN) in addition to an access key ID and secret access key. In this authentication scenario, temporary security credentials are used to connect to AWS Secrets ManagerAWS Secret Manager or AWS database services.

- [Authenticating by using IAM Role for AWS Secrets Manager](#)
- [Authenticating by using IAM Role for AWS database service](#)

# Authenticating by using IAM Role for AWS Secrets Manager

## About this task

Learn how to connect to AWS Secrets Manager using IAM role.

## Procedure

1. Log in to the Amazon AWS management console and ensure that you are connected to the relevant data center.
2. Click Services. Then, from the Security, Identity, & Compliance menu, select IAM.
3. From the menu, select Roles and then click Create role.
4. Under Common use cases, select EC2. Click Next: Permissions, then click Next: Tags, and then click Next: Review.
5. In the Role name field, enter the role name that you want to create. Example: to create role for *Guardium\_AWS\_Secret\_Manager\_Role*
6. Click Create role to create the Role ARN. Your Role ARN appears in the following format: *arn:aws:iam:<AWS Account ID>:instance-profile/<Role name>*.
7. Click Attach policies and then click Create policy to create three policies to integrate your Guardium® system with the AWS Secrets Manager. You can use the visual editor or JSON to add your code.

- a. Create a policy to assume role.

Example code:

```
Secret-mgr-assume-role-policy
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "VisualEditor0",
 "Effect": "Allow",
 "Action": "sts:AssumeRole",
 "Resource": "arn:aws:iam::role/*"
 }
]
}
```

Click Review policy and save the policy. The policy appears in the following format: *arn:aws:iam:<AWS Account ID>:policy/<policy-name>*

- b. Create a second policy to list the secret manager service to read secrets for all resources.

Example code:

```
Secret-mgr-read-all-secret-policy
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "VisualEditor0",
 "Effect": "Allow",
 "Action": "secretsmanager:GetSecretValue",
 "Resource": "arn:aws:secretsmanager:*:01234567901:secret:*
```

In the example, 01234567901 indicates the AWS account number. The wildcard *secret:\** indicates that all secrets are read.

Click Review policy and save the policy. The policy appears in the following format: *arn:aws:iam:<AWS Account ID>:policy/<policy-name>*

8. Define the trust relationship for the secret user by accessing Services->Identity and Access Management (IAM)->Roles. Select the role, click Trust relationships, then click Edit trust relationship and enter the code to create a trust relationship. Example:

```
Trust relationship
{
 "Version": "2012-10-17",
```

```

 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "AWS": [
 "arn:aws:iam::01234567901:role/Test1_Guardium_AWS_Secret_Manager_Role",
 "arn:aws:iam::01234567901:role/Test2_Guardium_AWS_Secret_Manager_Role",
 "arn:aws:iam::01234567901:user/nameofuser",
],
 "Service": "ec2.amazonaws.com"
 },
 "Action": "sts:AssumeRole"
 }
]
}

```

In the example, `01234567901` indicates the AWS account number and `nameofuser` is the username that is used to login to the AWS account.

Include the lines `arn:aws:iam::01234567901:role/Test1_Guardium_AWS_Secret_Manager_Role` or `arn:aws:iam::01234567901:role/Test2_Guardium_AWS_Secret_Manager_Role` in your code only when you use IAM instance profile and you want the roles to assume an alternate role.

In the example, `Test1_Guardium_AWS_Secret_Manager_Role` and `Test2_Guardium_AWS_Secret_Manager_Role` are the rolenames that are allowed to assume an alternate role `Guardium_AWS_Secret_Manager_Role`.

Review the code and click Update trust policy.

## What to do next

Note the following information:

- The access key ID and the secret access key for the secret user.
- The role ARN that is created in step [6](#).

This information is used to configure the AWS Secrets Manager on your Guardium system.

## Authenticating by using IAM Role for AWS database service

### About this task

12.1 and later Learn how to connect to AWS database services by using IAM role.

### Procedure

- Log in to the Amazon AWS management console and make sure that you are connected to the relevant data center.
- Click Services. Then, from the Security, Identity, & Compliance menu, select IAM.
- From the menu, select Roles and then click Create role.
- Under Common use cases, select EC2. Click Next: Permissions, then click Next: Tags, and then click Next: Review.
- In the Role name field, enter the role name that you want to create. Example: to create role for `Guardium_AWS_<databaseName>_Role`
- Click Create role to create the Role ARN. Your Role ARN appears in the following format: `arn:aws:iam:<AWS Account ID>:instance-profile/<Role name>`.
- Click Attach policies and then click Create policy to create three policies to integrate your Guardium® system with AWS database services. You can use the visual editor or JSON to add your code.

- Create a policy to assume role.

Example code:

```

Database-assume-role-policy
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "VisualEditor0",
 "Effect": "Allow",
 "Action": "sts:AssumeRole",
 "Resource": "arn:aws:iam::*:role/*"
 }
]
}

```

Click Review policy and save the policy. The policy appears in the following format: `arn:aws:iam:<AWS Account ID>:policy/<policy-name>`

- Create a second policy with the minimum access permissions required to run VA tests for your AWS database services.

Example code for DynamoDB:

```

DynamoDB-VA-policy
{
 "Sid": "VisualEditor0",
 "Effect": "Allow",
 "Action": [
 "dynamodb:DescribeTable",
 "dynamodb:GetResourcePolicy",
 "dynamodb>ListTables",
 "dynamodb>ListStreams",
 "dynamodb>CreateTable",
 "dynamodb>DeleteTable",
 "dynamodb:DescribeContinuousBackups",
]
}

```

```

 "cloudtrail>ListTrails",
 "cloudtrail>GetEventSelectors",
 "iam>ListEntitiesForPolicy"
],
 "Resource": "arn:aws:secretsmanager:*:01234567901:secret:*
```

Click Review policy and save the policy. The policy appears in the following format: `arn:aws:iam:<AWS Account ID>;policy/<policy-name>`

8. Define the trust relationship for the secret user by accessing Services > Identity and Access Management (IAM) > Roles. Select the role, click Trust relationships, then click Edit trust relationship and enter the code to create a trust relationship. Example:

```

Trust relationship
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "AWS": [
 "arn:aws:iam::01234567901:role/Test1_Guardium_AWS_Database",
 "arn:aws:iam::01234567901:user/nameofuser",
],
 "Service": "ec2.amazonaws.com"
 },
 "Action": "sts:AssumeRole"
 }
]
}
```

In the example, `01234567901` indicates the AWS count number and `nameofuser` is the username that is used to login to the AWS account.

Include the lines `arn:aws:iam::01234567901:role/Test1_Guardium_AWS_Database_Role` in your code only when you use IAM instance profile and you want the roles to assume an alternate role.

In the example, `Test1_Guardium_AWS_Database` is the rolename that is allowed to assume an alternate role `Guardium_AWS_<databaseName>_Role`.

Review the code and click Update trust policy.

## What to do next

---

Note the following information:

- The access key ID and the secret access key for the secret user.
- The role ARN that is created in step [6](#).

This information is used to configure the AWS Secrets Manager on your Guardium system.

## Authenticating by using IAM instance profile

---

You can authenticate by using the IAM instance profile only when you use a Guardium instance that is deployed on AWS EC2.

### Before you begin

---

Create the IAM role, the related policies, and obtain the Role ARN. For more information, see [Authenticating by using IAM Role](#).  
Note:

- When you configure the IAM instance profile for the AWS Secrets Manager on your Guardium system, you can use the Role ARN that is assigned on the AWS Secrets Manager or optionally use an alternate Role ARN.
- To monitor streams by using different IAM roles, create an account for each IAM role.

### Procedure

---

1. Log in to the Amazon AWS management console and ensure that you are connected to the relevant data center.
2. Access Services > Compute > EC2.
3. Under Resources, click Running instances.
4. Select the Guardium® EC2 image.
5. Access Action > Instance settings > Attach/Replace IAM Role.
6. From the IAM Role drop down, select the Role ARN that you created for the IAM Role configuration.

## What to do next

---

Configure the AWS Secrets Manager on your Guardium system.

## Configuring the AWS Secrets Manager on your Guardium system

---

Configure the AWS Secrets Manager on your Guardium® system. Each secret user must be configured on your Guardium system to access the AWS Secrets Manager.

## Before you begin

---

Make sure that you have the access key ID, the secret access key, and the Role ARN, if applicable, for your secret user. For more information, see [Selecting the authentication type and setting up roles](#).

## Procedure

---

1. Access Setup> Tools and Views> AWS Secret Manager Configurations.  
12.1 and later Access Setup> Tools and Views > AWS Authentication Configuration.
2. Click  to open the Create New AWS Secret Manager Configuration dialog.  
12.1 and later Click  to open the Create New AWS Authentication Configuration dialog.
3. In the Name field, enter an arbitrary name for the configuration. This name is used to configure your Guardium datasources to access the AWS Secrets Manager.
4. 12.1 and later Select the Secrets Manager checkbox.
5. In the Secret key for username field, enter the exact value of the Secret Key label for the *username* field that is specified in your AWS Secrets Manager Secret value vault. If the label for *username* is defined by the user, enter the user-defined value. The default value is *username*.
6. In the Secret key for password field, enter the exact value of the Secret Key label for the *password* field that is specified in your AWS Secrets Manager Secret value vault. If the label for *password* is defined by the user, enter the user-defined value. The default value is *password*.  
12.1 and later  
Note: If you do not select the Secrets Manager check box, ignore step 5 and step 6.
7. Select the Authentication type for your secret user. For more information on authentication types, see [Selecting the authentication type and setting up roles](#).
8. Depending on the type of authentication that you select, enter the AWS access key ID, the AWS secret access key ID, and the Role ARN.  
Note:
  - When you configure the IAM instance profile for the AWS Secrets Manager on your Guardium system, you can use the Role ARN that is assigned on the AWS Secrets Manager or optionally use an alternate Role ARN.
  - To monitor streams by using different IAM roles, create an account for each IAM role.
9. Click Save to save the configuration.

## What to do next

---

Note the name of your configuration. This information is used when you define your datasources to retrieve credentials from the AWS Secrets Manager.

Previous topic: [Selecting the authentication type and setting up roles](#)

Next topic: [Defining Guardium datasources to access AWS Secret Manager](#)

## Related reference

---

- [API to create an AWS Secrets Manager configuration](#).
- [API to list AWS Secrets Manager configurations](#).
- [API to update an AWS Secrets Manager configuration](#).
- [API to delete an AWS Secrets Manager configuration](#).

## Defining Guardium datasources to access AWS Secret Manager

---

Configure the datasources on your Guardium® system for automatic password provisioning using the AWS Secrets Manager. You can create a new datasource definition or edit an existing definition.

## Before you begin

---

Ensure that you gathered the following information:

- The name of the AWS Secrets Manager configuration. For more information, see [Configuring the AWS Secrets Manager on your Guardium system](#).
- The secret name. For more information, see [Creating a secret key](#).
- The location of your AWS data center, hostname, port number, and service name. For more information, see [Gathering required information from AWS Secrets Manager](#).

## Procedure

---

1. To access an existing datasource definition, go to Setup> Tools and Views> Datasource Definitions, and click . To create a new datasource definition, see [Creating a datasource definition](#).
2. Configure the Credential type by selecting the External password radio button.
3. In the External password type Location drop-down, select AWS Secrets Manager.
4. In the AWS Secrets Manager config drop-down, select the name of the AWS Secrets Manager configuration.
5. In the Secret name field, enter the secret name that you created on your AWS management console.
6. Enter the Region location of your data center that is configured on your AWS management console.
7. Enter the Host name/IP, Port number, and Service name that you gathered from your AWS management console.
8. Click Save and Test connection to ensure that the Guardium system can connect to the AWS Secrets Manager and fetch the datasource credential.

## What to do next

---

Repeat steps [2](#) to [8](#) to configure all your Guardium datasources to access the AWS Secrets Manager.

## Managing datasource credentials with HashiCorp

Integrate your Guardium® system with HashiCorp to securely store, manage, rotate, and retrieve credentials for all supported datasources.

You can configure your Guardium system to authenticate to the HashiCorp vault by using a username and password with no Transport Layer Security (TLS), server-side authentication with TLS, or client-side authentication with TLS. If you use client-side authentication with TLS, you must create and import a client signed certificate on all your systems such as the central manager and managed units, if any.

### 1. Gathering required information from HashiCorp

Obtain the HashiCorp configuration information from your HashiCorp administrator.

### 2. Creating a HashiCorp Policy

The HashiCorp administrator must create a policy that contains the permissions that are required to read and list the credentials and roles from the HashiCorp vault.

### 3. Creating and importing a client certificate

If you are using client-side authentication with TLS to access the HashiCorp vault, you must create and import a client certificate on all your systems such as the central manager and managed units.

### 4. Configuring HashiCorp on your Guardium system

Configure your Guardium system to access the HashiCorp vault and retrieve datasource credentials.

### 5. Defining Guardium datasources to access the HashiCorp vault

Configure the datasources on your Guardium system for automatic password provisioning by using HashiCorp. You can create a new datasource definition or edit an existing definition.

---

## Gathering required information from HashiCorp

Obtain the HashiCorp configuration information from your HashiCorp administrator.

## Before you begin

Ensure that the HashiCorp administrator has set up and configured the following items for your HashiCorp vault.

- Secrets: the default path or the custom path to the datasource credentials.
- Access: the authentication method and policy information
- Policies: the permissions that include static or dynamic credentials, roles, and configuration information for client web certificates. For more information on creating a policy, see [Creating a HashiCorp Policy](#).

## Procedure

Gather the following information from your HashiCorp administrator.

- The role name that is unique to your datasource.
- The custom path to your datasource credentials, if any.
- The hostname and IP address for your database, if applicable.
- The port number for your database.
- The database name.

Next topic: [Creating a HashiCorp Policy](#)

---

## Creating a HashiCorp Policy

The HashiCorp administrator must create a policy that contains the permissions that are required to read and list the credentials and roles from the HashiCorp vault.

## Procedure

The following is an example of a policy with the minimum amount of privilege that is required to access the vault.

```
Permissions to dynamic roles and creds for different paths
path "database/creds/*" {
 capabilities = ["read", "list"]
}

Permissions to dynamic roles and creds for different paths
path "database/roles/*" {
 capabilities = ["read", "list"]
}

Permissions to static roles and creds for different paths
path "database/static-creds/*" {
 capabilities = ["read", "list"]
}

Permissions to static roles and creds for different paths
```

```

path "database/static-roles/*" {
 capabilities = ["read", "list"]
}

Permissions to dynamic roles and creds for different paths
path "custom/123/abc123/databases/mongo/mongo123/creds/*" {
 capabilities = ["read", "list"]
}

Permissions to dynamic roles and creds for different paths
path "custom/123/abc123/databases/mongo/mongo123/roles/*" {
 capabilities = ["read", "list"]
}

Permissions to static roles and creds for different paths
path "custom/123/abc123/databases/mongo/mongo123/static-creds/*" {
 capabilities = ["read", "list"]
}

Permissions to static roles and creds for different paths
path "custom/123/abc123/databases/mongo/mongo123/static-roles/*" {
 capabilities = ["read", "list"]
}

Configure for client web certificates
path "auth/*" {
 capabilities = ["read"]
}

```

Previous topic: [Gathering required information from HashiCorp](#)  
 Next topic: [Creating and importing a client certificate](#)

---

## Creating and importing a client certificate

If you are using client-side authentication with TLS to access the HashiCorp vault, you must create and import a client certificate on all your systems such as the central manager and managed units.

### Procedure

1. On your Guardium® system, create a certificate signing request (CSR) file by using the CLI command **create csr alias**.

Copy the CSR starting at the '----BEGIN NEW CERTIFICATE REQUEST----' tag and ending at the '----END NEW CERTIFICATE REQUEST' tag.

Provide the CSR file to a Certificate Authority (CA) of your choice to obtain a valid certificate. The certificate must be in PEM format to import into your Guardium system. After you receive the PEM certificate from your CA, import the certificate by using the CLI command **store certificate keystore alias**.

Example:

```

create csr alias

Please enter a one-word alias to uniquely identify this certificate:
vault

If the Common Name (CN=) field is used as an Identifier, prefix the identifier with ID: (example ID:1234).

What is the Common Name (CN=) for this certificate (default: gmachine.com) ?

What is the name of your organizational unit (OU=) ? YourTeam

What is the name of your organization (O=) ? YourCompany

What is the name of your city or locality (L=) ? YourCity

What is the name of your state or province (ST=) ? YourState

What is the two-letter country code for this unit (C=) ? US

What encryption algorithm should be used?
1=dsa
2=rsa
3=ecdsa
Default: RSA

Invalid input or no input. Using default 'RSA'

What is the keysize to use (1=1024 or 2=2048. Default '2048') ?
Invalid input or no input. Using default '2048'

Add up to 99 optional SANs (Subjective Alternative Name) in fully qualified domain name format. To continue without adding
a SAN, press Enter.

What is the name of SAN #1 ?

Generating CSR...

Certificate Request:
Data:
Version: 0 (0x0)

```

```
Subject: C=US, ST=YourState, L=YourCity, O=YourCompany, OU=YourTeam, CN=gmachine.com
```

```
-----BEGIN NEW CERTIFICATE REQUEST-----
```

```
#####
#####
```

```
-----END NEW CERTIFICATE REQUEST-----
```

```

```

```
store certificate keystore alias
```

```
ok
```

- On the Guardium system that contains the CA certificate, copy the CSR file to the database server to have it sign with a CA root certificate.  
Example:

```
openssl x509 -req -in gmachine_signing_request.csr -CA ca_root_certificate.crt -CAkey ca_private_key.key -CAcreateserial -out gmachine_signed_certificate.crt -days 10000 -sha256
```

- Configure the HashiCorp vault with the new trusted client certificate that is allowed to authenticate.

Example:

```
[root@Hashicorp ssl]# vault write auth/cert/certs/gmachine \
 display_name=gmachine \
 policies=guardium_policy \
 certificate=@gmachine_signed_certificate.crt \
 ttl=3600
Success! Data written to: auth/cert/certs/gmachine
```

- Store the signed client certificate that is sent back from the database server into the tomcat.keystore of your Guardium system.

If the client certificate is signed by a self-sign CA certificate, then you must also upload the CA certificate along with the signed client certificate.  
Example to import both the CA certificate and the signed client certificate together:

```
store certificate keystore alias console
```

```
Please enter a one-word alias to uniquely identify this certificate:
vault
```

```
Found the following Certificate Signing Request (CSR):
```

```

```

```
Certificate Request:
```

```
Data:
```

```
Version: 0 (0x0)
```

```
Subject: Subject: C=US, ST=YourState, L=YourCity, O=YourCompany, OU=YourTeam, CN=gmachine.com
```

```
-----BEGIN NEW CERTIFICATE REQUEST-----
```

```
#####
#####
```

```
-----END NEW CERTIFICATE REQUEST-----
```

```

```

```
Are you importing a certificate that corresponds to this CSR? [y/N]
```

```
y
```

```
Please paste your End-Entity certificate below in PEM encoded format. A certificate in
PEM encoded format should include the '-----BEGIN CERTIFICATE-----' and '-----END
CERTIFICATE-----' tags. The Certificate Authority (CA) Root and Intermediate
certificate(s) (if applicable) will also need to be pasted at this time for
validation purposes. Please ensure that all certificates are in PEM format and
include the aforementioned tags. When pasting multiple certificates, please make
sure that each certificate is pasted on a new line in the following order:
```

```
-----BEGIN CERTIFICATE-----
(End-Entity certificate)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Intermediate certificate(s) - if applicable)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Root certificate)
-----END CERTIFICATE-----
```

```
Once done pasting your certificate(s), press ENTER followed by CTRL-D to continue.
```

```
-----BEGIN CERTIFICATE-----
```

```
#####
#####
```

## Configuring HashiCorp on your Guardium system

Configure your Guardium® system to access the HashiCorp vault and retrieve datasource credentials.

## Before you begin

If you are using client-side authentication with TLS, create and import a client certificate on all your systems including the central manager and managed units. For more information, see [Creating and importing a client certificate](#).

## About this task

Use the following procedure to configure your Guardium system to access the HashiCorp vault by using the Guardium UI.  
Note: Create this configuration only on your central manager or stand-alone system.

## Procedure

1. Access Setup > Tools and Views > HashiCorp Configurations.
  2. Click  to open the Create New HashiCorp Vault Access Configuration dialog.
  3. In the Name field, enter a name for the HashiCorp configuration.
  4. Select the Authentication type for the configuration. You can authenticate to the HashiCorp vault by using a username and password with no TLS, server-side authentication with TLS, or client-side authentication with TLS.
  5. Enter the HashiCorp vault hostname.
  6. Enter the HashiCorp vault port number.
  7. Depending on the type of authentication, enter the username, password, and select the Use TLS option, if applicable:
    - If the authentication type is Username & Password without TLS, enter the username and password. Do not check Use TLS.
    - If the authentication type is Username & Password with server-side authentication, enter the username and password. Then, check Use TLS.
    - If the authentication type is TLS Certificates with client-side authentication, check Use TLS and import the client signed certificate if you haven't already.
  8. Save and Test connection.

## What to do next

Note the name of your configuration. This information is used when you define your datasources to retrieve credentials from the HashiCorp vault.  
Important: If you rebuild your Guardium system, you must delete any related TLS certificates from the HashiCorp vault. Then, create and import the client certificates again.

**Previous topic:** [Creating and importing a client certificate](#)  
**Next topic:** [Defining Guardium datasources to access the HashiCorp vault](#)

## Related reference

- [API to create a HashiCorp configuration.](#)
  - [API to delete a HashiCorp configuration.](#)
  - [API to list HashiCorp configurations.](#)
  - [API to update a HashiCorp configuration](#)

- [API to test a HashiCorp configuration.](#)

## Defining Guardium datasources to access the HashiCorp vault

Configure the datasources on your Guardium® system for automatic password provisioning by using HashiCorp. You can create a new datasource definition or edit an existing definition.

### Procedure

1. To access an existing datasource definition, go to **Setup > Tools and Views > Datasource Definitions**, and click . To create a new datasource definition, see [Creating a datasource definition](#).
2. Configure the Credential type by selecting the External password radio button.
3. In the External password type drop-down, select HashiCorp.
4. In the HashiCorp configuration drop-down, select the name of the HashiCorp configuration.
5. In the Role field, enter role name for the datasource that is created by the HashiCorp administrator .
6. Enter the Path if the HashiCorp administrator created a custom path to access the datasource credentials.
7. Enter the Host name/IP, Port number and Database information for the datasource if it has not been configured already.
8. Click Save and Test connection to ensure that the Guardium system can connect to the HashiCorp vault and fetch the datasource credential.

### What to do next

Repeat steps [2](#) to [8](#) to configure all your Guardium datasources to access the HashiCorp vault.

**Previous topic:** [Configuring HashiCorp on your Guardium system](#)

## Database Auto-discovery

The Auto-Discovery application scans and probes your servers for open ports to prevent unknown or unwanted connections to your network. You can run auto-discovery processes on demand, or schedule the processes on a periodic basis.

### Database Auto-discovery Overview

There are many scenarios where databases can exist undetected on your network and expose your network to potential risk. Old databases might be forgotten and unmonitored, or a new database might be added as part of an application package. A rogue DBA might also create a new instance of a database to conduct malicious activity outside of the monitored databases.

Auto-discovery uses scan and probe jobs to ensure that no database goes undetected in your environment.

- A *scan* job scans each specified host (or hosts in a specified subnet), and compiles a list of open ports that are specified for that host.
- A *probe* job uses the results of the scan to determine whether there are database services that are running on the open ports. A probe job cannot be completed without first running a scan. View the results of this job in the Databases Discovered predefined report.

Follow these steps to use the Auto-discovery application:

1. Create an Auto-discovery process to search specific IP addresses or subnets for open ports.
2. Run the Auto-discovery process on demand or on a scheduled basis.
3. View the results of the process with Auto-discovery reports, or create custom reports.

Auto discovery has its own processes that are independent of audit processes, but they work exactly the same way as audit processes.

You can only enter IPs when doing a scan, you cannot enter host names. However, Guardium does detect host names as part of the report. Guardium does not truncate host names in the Guardium product. However, it may be necessary to configure the report to have wider columns.

Guardium auto-discovery does not guess about databases that appears during a probe. If Guardium auto-discovery says it has found a database, then it is 100% certain what the database is.

Attention: Database auto-discovery works with the following databases:

- Db2
- Informix
- MongoDB
- Microsoft SQL Server
- MySQL
- Netezza
- Oracle
- PostgreSQL
- SAP HANA
- Sybase
- Teradata

Auto-discovery only finds running databases. Databases need to be started if discovery is to be used during the installation. Due to how the AIX KTAP interception works, the databases need to be restarted after the first time S-TAP runs. If the databases are not restarted, some interception does not work.

## Create an Auto-discovery Process

Specify which host and ports the Auto-discovery process scans.

1. Configure Auto-discovery by clicking Discover > Database Discovery > Auto-discovery Configuration.
2. Click New to create a new process and open the Auto-discovery Process Builder.
3. Enter a Process name that is unique on your Guardium® system.
4. To run a probe job immediately after the scan job completes, check the Run probe after scan check box.
5. To scan for open ports on hosts where discovery is blocked, check the Skip host discovery check box.  
Note: Host discovery requires ports 80 and 443. If those ports are blocked, using Skip host discovery forces scanning for open ports on those hosts. This is equivalent to `nmap -Pn`.
6. For each host or subnet to be scanned, enter the host and port, and click Add scan. Each time that you add a scan, it is added to the task list.  
Note:
  - Wildcard characters are enabled. For example: to select all addresses beginning with 192.168.2, use 192.168.2.\*.
  - Specify a range of ports by putting a dash between the first and last port numbers in the range. For example: 4100-4102.
  - After you add a scan, modify the host or port by typing over it. Click Apply to save the modification.
  - If you have a dual stack configuration, you will need to set up a scan for both the IPv4 and the IPv6 addresses.
  - To remove a scan, click the Delete this task icon for the scan. If a task has scan results dependent upon it, the scan cannot be deleted.
7. When finished adding scans, click Apply, and run the job or schedule the job in the future.

See [Scheduling](#) if you need help defining a schedule.

## Run or Schedule an Auto-discovery Process

---

Run or schedule scan and probe jobs as part of the Auto-discovery process.

1. Click Discover > Database Discovery > Auto-discovery Configuration.
2. Select the process to-be run from the Auto-discovery Process Selector list and do one of the following:
3.
  - To run a job immediately, click Run Once Now.
  - To schedule a job in the future, click Modify Schedule (see [Scheduling](#) if you need help defining a schedule).  
Note: A probe job cannot run without the results of the scan job. You can schedule the two jobs to run individually, or you configure the probe job to run after the scan job by modifying a process, and checking the Run probe after scan check box.
4. After you start or schedule a job, you can click Progress Summary to display the status of this process.

## Auto-discovery Reports

---

Open the Auto-discovery reports by clicking Discover > Reports and selecting from the available reports.

You can create custom reports with the Auto-discovery Query Builder. Open the Auto-discovery Query Builder by clicking Discover > Database Discovery > Auto-discovery Query Builder.

## Databases Discovered Report

---

Open the Databases Discovered report by clicking Discover > Reports > Databases Discovered.

The main entity for this report is the Discovered Port. Each individual port that is discovered has its own row in the report. The columns that are listed are: Time Probed, Server IP address, Server Host Name, DB Type, Port, Port Type (usually TCP), and a count of occurrences.

There are no special runtime parameters for this report, but it excludes any discovered ports with a database type of Unknown.

When an auto-discovery process definition changes, the statistics for that process are reset.

## Auto-discovery Tracking Domain

---

The Auto-discovery Tracking domain contains all of the data reported by Auto-discovery processes. Click any entity name to display its attributes.

Auto-discovery Tracking Domain Entities

- Auto-discovery Scan provides a time stamp for each scan operation.
- Discovered Host provides the IP address and host name for each discovered host.
- Discovered Port provides a time stamp, identifies the port, and provides the database type for each port discovered open.

## Cloud database service protection

---

Protect your cloud databases by using data activity stream monitoring or by using native audit.

### Cloud database service protection for Amazon AWS with data streams

---

After you define a cloud DB service account with an audit type of Data Streams, you can use cloud database service protection with data streaming to monitor AWS data streams from selected Guardium collectors. For more information, see [Cloud database service protection Amazon AWS setup](#).

### Cloud database service protection for Azure event hubs

---

After you define a cloud DB service account with an audit type of Data Streams, you can use cloud database service protection with data streaming to monitor Azure event hubs from selected Guardium collectors. For more information, see [Cloud database service protection Azure setup](#).

## Cloud database service protection with native audit

---

Cloud database protection provides classification, vulnerability assessment, and object auditing on cloud databases, using the native audit. For more information, see [Cloud database service protection workflow](#)

- [Cloud database service protection Amazon AWS setup](#)

You can use AWS database activity monitoring to provide cloud database service protection with Guardium. Before you can define a Guardium cloud DB service account, you need to perform a few setup steps.

- [Cloud database service protection Azure setup](#)

Use database activity monitoring to provide cloud database service protection for Azure event hubs.

- [Cloud database service protection with native audit](#)

Cloud database protection provides classification, vulnerability assessment, and object auditing on cloud databases, using the native audit.

---

## Cloud database service protection Amazon AWS setup

You can use AWS database activity monitoring to provide cloud database service protection with Guardium®. Before you can define a Guardium cloud DB service account, you need to perform a few setup steps.

Note: AWS supports data activity monitoring only for new clusters.

### Create an Amazon RDS cluster

---

To use database activity monitoring, create an Amazon RDS cluster that uses Aurora PostgreSQL-compatible with PostgreSQL 10.7 database engine.

Take the following steps to create the Amazon RDS cluster:

1. From your AWS account, create a new KMS key (do not use the default KMS key).
2. Create an Amazon RDS cluster in a region that supports data activity monitoring (DAS).
3. Wait until the cluster and instances are created before you enable the database activity monitoring.

Note: Note the following limitations on database activity monitoring traffic:

- The following rules and policies are not supported:
  - Returned data and extrusion rules
  - Policies that interact with S-TAP (such as S-GATE, Ignore, Terminate)
  - SQL errors (AWS limitation)
- Audit data is processed in the order that it was received
- If more than one Guardium collector consumes from a stream, traffic is randomly distributed (because each collector has a different session ID)

## Define the AWS Identity and Access Management policy

---

Define the Identity and Access Management (IAM) policy for your AWS account as described in [Define AWS IAM for data streams](#).

After you create the Amazon RDS cluster and define the AWS IAM policy, you can define a Guardium cloud DB service account, as described in [Define, modify, and delete AWS cloud DB service accounts](#).

- [Define AWS IAM for data streams](#)

Define the Identity and Access Management (IAM) policy for your Amazon Web Services (AWS) account, depending on the required permissions.

- [Define, modify, and delete AWS cloud DB service accounts](#)

Define a Guardium cloud DB service account for Amazon AWS with your database credentials, and modify or delete the cloud DB service account.

- [Discover and configure AWS data streams](#)

Discover data streams in the AWS cloud account, and assign data streams to Guardium collectors.

- [Manage AWS data streams](#)

Manage and troubleshoot AWS data streams.

---

## Define AWS IAM for data streams

Define the Identity and Access Management (IAM) policy for your Amazon Web Services (AWS) account, depending on the required permissions.

The minimum IAM permissions for data streams include viewing the configuration and changing tags. The following JSON example defines the minimum permissions that you need to run cloud database service protection. You can use the sample JSON (or create your own) with the following changes:

- For the values in the Resource parameter, change the account portion of the Amazon Resource Name (ARN) to your account.
- For the KMS resource, change to the key that you used to create the database activity stream. If your site has multiple keys, you can set the key to the \* (asterisk) wildcard.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "kinesis>ListStreams",
 "cloudwatch:PutMetricData",
 "cloudwatch:GetMetricStatistics"
],
 "Resource": "*"
 }
]
}
```

```

},
{
 "Effect": "Allow",
 "Action": [
 "kinesis:RegisterStreamConsumer",
 "kinesis:DescribeStreamConsumer",
 "kinesis>ListStreamConsumers",
 "kinesis:DescribeStreamSummary",
 "kinesis:DescribeStream",
 "kinesis:GetShardIterator",
 "kinesis:GetRecords",
 "kinesis>ListShards",
 "kinesis:SubscribeToShard"
],
 "Resource": "arn:aws:kinesis::stream/*"
},
{
 "Effect": "Allow",
 "Action": [
 "kms:Decrypt"
],
 "Resource": "*"
},
{
 "Effect": "Allow",
 "Action": [
 "dynamodb>CreateTable",
 "dynamodb:DescribeTable",
 "dynamodb:GetItem",
 "dynamodb:PutItem",
 "dynamodb:Scan",
 "dynamodb:UpdateItem",
 "dynamodb>DeleteItem"
],
 "Resource": "arn:aws:dynamodb::table/*"
}
]
}

```

## Define, modify, and delete AWS cloud DB service accounts

Define a Guardium cloud DB service account for Amazon AWS with your database credentials, and modify or delete the cloud DB service account.

### Define a Guardium cloud DB service account

#### About this task

Create cloud accounts to manage the connection between your AWS cloud databases and Guardium.

#### Procedure

1. Browse to Discover > Database Discovery > Cloud DB Service Protection.
2. Click  to open the Create Cloud DB Service Account Definition window.
3. Define the account:
  - Name: An account name that is unique to your site.
  - Provider: Select Amazon as the provider name from the menu.
  - Audit type: Select Data Streams to use AWS database activity monitoring. If Audit type does not display, then you must enable access to data streams. For more information, see [enable\\_datastream](#).
  - Authentication type: Depending on the authentication type that you select, provide the requested information. The authentication types are:
    - Security Credentials: Select to specify user-based credentials to manage AWS access.
    - IAM Role: Select to use IAM roles to manage to your AWS access.
    - To monitor streams using different IAM roles, create an account for each IAM role.
  - IAM Instance Profile: Select when your Guardium instance is on EC2 and the EC2 instance has an attached IAM role with configured policies.  
Note: To use an IAM instance profile, the central manager and all collectors must be on EC2 and configured with an instance profile.

Depending on the configuration, the Authentication type can include the following options:

  - AWS access key ID and AWS secret access key ID: Supplied by Amazon.
  - Role ARN: The Amazon resource name (ARN) for the permissions that are assigned when you define the AWS IAM (as described in [Define AWS IAM for data streams](#)).
4. Click Create.

The account is created and the Cloud DB Service Accounts list updates with the new Cloud account.

#### What to do next

Discover and start monitoring the data streams. For more information, see [Discover and configure AWS data streams](#).

### Modify a cloud DB service account

You can modify all parameters except the provider.

#### Procedure

1. Select the cloud account under Cloud DB Service Accounts, and click in the right pane.
2. Modify the configuration.
3. Click Save.

## Delete a cloud DB service account

---

When you delete a cloud DB service account, Guardium no longer monitors database activity.

### Procedure

1. Select the account in the Cloud DB Service Accounts pane and click
2. From the Confirmation window, click Yes to delete the account or No to cancel the deletion.

## Discover and configure AWS data streams

---

Discover data streams in the AWS cloud account, and assign data streams to Guardium collectors.

### About this task

---

After you define your Guardium cloud DB service account for Amazon AWS, you can discover available data streams and assign them to Guardium collectors.

### Procedure

---

1. Browse to Discover > Database Discovery > Cloud DB Service Protection, and click the name of a Cloud DB service account. The Cloud DB Service Account page opens, and displays the Discover Streams table.  
Note: The next time that you access the Cloud DB Service Account page, the table is closed. Click Discover Streams to reopen the table.
2. Select the row of each region whose streams you want to discover and click Discover.  
Optionally, use the filter to limit your search. For example, type us into the filter window to show only data streams that contain the letters "us." Guardium searches the regions, and adds any new streams from the selected regions to the Streams table.
3. Scroll down to the Streams table (or click Hide Discover Streams).
4. Select a stream and then click Assign Collector to open the Assign Collector to Selected Stream window. Enter the following information:
  - Collector: Select one or more collectors from the Select collector list.  
Note: You can assign collectors only to the central manager (in a managed environment).
  - DB Type: The database type.
  - DB DNS endpoint: Your DB DNS endpoint.
  - Port: The DB DNS endpoint port.
  - Cluster resource ID: Required. The cluster resource ID for the AWS RDS cluster associated with the stream. If you enter an invalid or unknown cluster resource ID, an error is reported in the status for the stream.
  - Consumer group name: Determines whether multiple consumers have a shared or separate view of this data stream. The consumer group name can be any unique name. To share the data stream view, use the same consumer group name.
5. Optionally, select Start monitoring stream. If you do not start monitoring now, you can enable monitoring from the Streams table later.

### What to do next

---

Select the stream and use Enable monitoring and Disable monitoring to turn monitoring of the selected stream on and off.  
Manage your data streams. For more information, see [Manage AWS data streams](#).

## Manage AWS data streams

---

Manage and troubleshoot AWS data streams.

After your data streams are enabled and running, you can use the Streams table to track and manage the data streams.

### The Status column

---

The Stream table Status column provides a quick view of the health of the data stream. The meaning of the status colors is as follows,

- Green - Good. The Comments column reads All Good.
- Blue - Not yet configured.
- Gray - Unavailable.
- Yellow - Warning. Usually, yellow status includes the message `consumerNoInboundRecords`, which indicates that the consumer received no records in the last 10 minutes. This status is usually okay. However, if you see a yellow status when your database is processing queries, then something might be configured incorrectly, most likely on the network or cloud side.
- Red - An error condition. The Comments column might contain useful information about why the error occurred.

Tip: Hover your mouse over a status spot to see a status description.

## Enable and disable monitoring

---

From the Streams header, you can enable or disable monitoring for individual streams.

- To start monitoring a stream, select a disabled stream and click Enable Monitoring.
- To stop monitoring a stream, select a running stream and click Disable Monitoring.

## View information about individual collectors

---

For central manager configurations, when a stream is enabled, the Stream column displays a small  icon. Click the  to show details about each collector. In the Monitor enabled column, you can turn individual collectors on and off.

## View status history

---

Select a stream and then click Status History to view the status history for this stream. The following information displays for each collector in the stream:

- Status from and Status to - The start and end times for this status history period. When the state changes, the status history period ends.
- Collector (for central manager configurations) - The collector for this status history period.
- Status - The state of the collector during this period.
- Comments - Notes about the status. When a collector fails, the Comments section often contains useful information about why the failure occurred.

## Filter stream data

---

From the Streams header, enter text into the Filter dialog. The Streams table displays any stream with text that matches the filter text; the remaining streams are hidden.

## Create a stream manually

---

While it is recommended that you discover streams, you can, if needed, add a stream manually, as follows:

1. In the Streams table, click  to open the Add a new stream dialog.
2. In the Add a new stream dialog, specify the required parameters from the AWS console:
  - Stream name - The name of the stream from the RDS cluster configuration.
  - Region - One of the regions from the Select region list.
  - Collector - Collectors that are assigned to the stream.
  - DB type - The database type for the stream.
  - DB DNS endpoint - Your DNS endpoint.
  - Port - The DB DNS endpoint port.
  - Cluster resource ID - The cluster resource ID from your AWS account.
  - Consumer group name - Determines whether multiple consumers have a shared or separate view of this data stream. The consumer group name can be any unique name. To share the data stream view, use the same consumer group name.

## Cloud database service protection Azure setup

---

Use database activity monitoring to provide cloud database service protection for Azure event hubs.

You can use database activity monitoring to provide cloud database service protection for Azure event hubs with Guardium®. Before you can define a Guardium cloud database service account for Azure, you need to set up your Azure account or gather information about your existing account.

Note:

- Cloud database service protection for Azure event hubs works with Microsoft Azure SQL Database, Azure SQL Managed Instance, and Microsoft Azure Cosmos DB.
- To use cloud database service protection with Azure, you need to be able to create Consumer Groups, which requires the Azure Standard Pricing Tier. You cannot use the \$Default Consumer Group.
- 12.1 and later For 12.1 and later versions of Guardium, you can configure a single Azure event hub for different Azure cloud databases of the same type.

Important: If you are using Azure SQL Managed Instance, you must enable logging at both the server and database levels before you define the cloud database service account.

1. Make sure that the ssh, 5671, and 5672 ports are open.
2. Use SQL Server Management Studio (SSMS) to set up and enable a Server Audit Specification that sends SQL Security Audit Events to the Event Hub.
3. From your managed database, set up and enable the Database Audit Specification.
4. On the Azure Managed Instance page, browse to Monitoring > Diagnostic Settings > Logs > Categories, and then select SQL Security Audit Event.

## Gathering Microsoft Azure information

---

To use database activity monitoring, you need the following information about each Microsoft Azure event hub that you want to monitor. These parameters are created when you configure an Azure event hub. For detailed information about configuring Azure, see the Microsoft Azure documentation. Find or create the following Azure parameters:

- Namespace: The Event Hubs namespace.
- Event Hub Name: Created from within the Event Hubs namespace.
- Shared access policy name and key: From the Event Hubs Namespace. To create a shared access policy, select *Event Hubs Name* > Shared Access Policy > *your policy name* to generate a shared access key.  
Note: Do not use the shared access policy in the Event Hub.  
Select Manage, Send, and Listen options for the Policy Name.
- Consumer Group Name: From the Event Hubs Instance page for the selected Event Hub. From Entities, select or create a Consumer Group.  
Notes:

If you use the same Consumer Group for multiple collectors, traffic is split between the collectors. If you create a Consumer Group for each collector, each collector gets its own copy of the traffic.

You cannot use the \$Default Consumer Group.

- Storage Connection String: Create a storage account (from the Azure dashboard) and then from Storage accounts, select Shared access signature to generate a shared access signature and connection string. The Storage account contains checkpoints for consumer progress in the Event Hubs partition. For example:

```
BlobEndpoint=https://mystoragename.blob.core.windows.net/;QueueEndpoint=https://mystoragename.queue.core.windows.net/;File
Endpoint=https://mystoragename.file.core.windows.net/;TableEndpoint=https://mystoragename.table.core.windows.net/;SharedAccessSignature=sv=2019-12-12&ss=bfqt&srt=scs&sp=rw&ldacupx&se=2025-09-16T00:54:06Z&st=2020-09-
15T16:54:06Z&spr=https&sig=q%2FTuyiJqkNgfdfgdfgzaNj3V7Y0cr2EbLqo16Hg%3D
```

Note: On the Shared access signature window, change the expiry end date to meet your requirements.

- Cluster resource Id: To find the cluster (or database) resource string:
  - For AzureSQL - From the Azure dashboard, browse to Properties > Resource ID.
  - For any Cosmos data source - The resource ID is the part of the URL that starts with /subscriptions and ends with the *data source name*. You can copy the resource ID from the URL, for example, if the URL for Microsoft Azure is:

```
https://portal.azure.com/#@company.onmicrosoft.com/resource/subscriptions/8333367e-1234-467d-b3fc-
5b78c5721df0/resourceGroups/rg1/providers/Microsoft.DocumentDb/databaseAccounts/ibmcosmostable1/overview
```

Then the Cosmos resource ID is:

```
/subscriptions/8333367e-1234-467d-b3fc-
5b78c5721df0/resourceGroups/rg1/providers/Microsoft.DocumentDb/databaseAccounts/ibmcosmostable1
```

12.1 and later For 12.1 and later versions of Guardium, you don't need to create the Azure parameter, Cluster resource Id.

After you create your account and have the necessary information, you can define the cloud DB service accounts that you need.

## Tips and tricks

- Before you start, create standard naming conventions to prevent later confusion. Consider including the name of the Event Hub and the name of the database that you are monitoring for each related element. For example, if the database name is **use1-db5**, use the following naming conventions:
  - Namespace: **use1-ehn1**
  - Shared Access: **use1-ehn1-sa1**
  - Event Hub: **use1-db5-ehn1-eh3**
  - Consumer Group: **use1-db5-ehn1-eh3-cg**
- From the Guardium collector, make sure that outbound ports 443 and 5671 are available for the connections between the collector and Azure Event Hub.
- When you create a namespace, consider selecting Enable Auto-Inflate.
- Cosmos databases do not use usernames. Therefore, usernames are never returned from Cosmos.
- To help debug database activity monitoring issues, use the **support store datastreams\_diag** and **support must\_gather datastreams\_issues** CLI commands. In general, use Support CLI commands only under the guidance of IBM Technical Support. For more information, see [Support CLI Commands](#).
- Safeguarding your storage connection string always is important because it contains sensitive data about your storage account. So, regularly regenerate your storage connection string to ensure the highest level of security for your storage. For more information about configuring storage connection strings, see the Azure Blob Storage documentation.
- Define, modify, and delete Azure cloud database service accounts**  
Define a Guardium cloud database service account for Azure with your database credentials, and modify or delete the cloud database service account.
- Monitor Azure event hubs**  
After you define your Guardium cloud DB service account for Azure, you can assign the Azure event hub to a Guardium collector for monitoring.
- Manage Azure event hubs**  
Manage and troubleshoot event hub monitoring from Guardium.

## Define, modify, and delete Azure cloud database service accounts

Define a Guardium cloud database service account for Azure with your database credentials, and modify or delete the cloud database service account.

### Define a Guardium cloud database service account

#### About this task

Create cloud accounts to manage the connection between your Azure event hubs and Guardium®.

#### Procedure

- Browse to Discover > Database Discovery > Cloud DB Service Protection.
- Click  to open the Cloud DB Service Account pane.
- To use database activity monitoring with data streams, select Data Streams as the Audit type. If Audit type does not display, then you must enable access to data streams. For more information, see [enable\\_datastream](#).
- Define the account:
  - Name: A name for this account.
  - Provider: Select Azure from the Provider menu.
- Configure the Azure account. From Azure Configuration, enter the following information:
  - Shared access policy name
  - Shared access policy key

For more information about the shared access policy name and key, see [Gathering Microsoft Azure information](#)

6. Click Create.  
The account is created and the Cloud DB Service Accounts list updates with the new cloud account.

## What to do next

Monitor event hubs. For more information, see [Monitor Azure event hubs](#).

## Modify a cloud DB service account

You can modify any parameters except the provider and audit type.

### Procedure

1. Select the cloud account under Cloud DB Service Accounts, and click in the right pane.
2. Modify the configuration.
3. Click Save.

## Delete a cloud DB service account

When you delete a cloud DB service account, Guardium no longer monitors database activity.

### Procedure

1. Select the account in the Cloud DB Service Accounts pane and click .
2. From the Confirmation window, click Yes to delete the account or No to cancel the deletion.

## Monitor Azure event hubs

After you define your Guardium cloud DB service account for Azure, you can assign the Azure event hub to a Guardium collector for monitoring.

## About this task

For Azure, Guardium monitors event hubs. To start monitoring event hubs, you need to take the following steps:

- In Azure, associate the event hub to the database you want to monitor.
- In Guardium, use the Event Hubs window to associate an Azure event hub with a Guardium collector.

## Procedure

From Azure, associate the event hub to your database.

1. From the Azure home page, take the following steps, depending on whether your site uses an Azure SQL Database or a Cosmos database.
  - For an Azure SQL Database:
    - Select SQL databases, and then select the database that you want to associate with Guardium.
    - Under Security, select Auditing.
    - Turn Auditing to ON.  
Note: Do not enable auditing on both the database and the server. Note that if you enable auditing on the server you will receive records for all databases on that server.
    - Under Audit log destination, select Event Hub (preview).
    - Select Event hub Configure and then configure the Event hub details by selecting the Event hub namespace, the Event hub policy name, and the Event hub name .
    - Click OK to save your changes.
  - For any supported Cosmos database:
    - Select Azure Cosmos DB, and then select the database that you want to associate with Guardium.
    - From Monitoring, open Diagnostic Settings
    - Click Add Diagnostic setting.
    - Select Event hub Configure and then configure the Event hub details by selecting the Event hub namespace, the Event hub policy name, and the Event hub name .
    - Under Logs, select DataPlaneRequests.
    - From Add Diagnostic setting, enter a name for this datastream and select Stream to event hub.
    - Click Save to save your changes.

Then, from Guardium, you can associate the Azure event hub with a Guardium collector:

2. In Guardium, browse to Discover > Database Discovery > Cloud DB Service Protection, and select a Cloud DB service account.  
The Cloud DB Service Account window opens, and displays the Event Hubs table.
3. From the Event Hubs window, click to open the Add a new event hub pane.
4. Enter the following information, which is described in [Gathering Microsoft Azure information](#):
  - Event Hub Name: The name of your Azure event hub.
  - Collector: The name or IP address of the Guardium collector.
  - Namespace: Your Azure event hub namespace.
  - DB Type: Select the database type for your data.
  - DB DNS endpoint: The DNS name of the database. For example, `mycosmostable1.table.cosmos.azure.com`.
  - Port: The DB DNS port.

- Consumer Group Name: The Azure consumer group name.
  - Storage Connection String: The Azure storage connection string.
  - Cluster resource id: The database resource ID for the data source.
- 12.1 and later For 12.1 and later versions of Guardium, you don't need DB DNS endpoint, Port, and Cluster resource Id for a new event hub pane.
5. Optionally, select Start monitoring event hub. If you do not start monitoring now, you can enable monitoring from the Event Hubs table later.

## What to do next

---

Select the event hub and use Enable monitoring and Disable monitoring to turn monitoring of the selected event hub monitoring on and off. Manage your event hubs. For more information, see [Manage Azure event hubs](#).

---

## Manage Azure event hubs

Manage and troubleshoot event hub monitoring from Guardium.

After you enable event hub monitoring, you can track and manage the event hubs and event hub streams from the Event Hubs table.

## The Status column

---

The Event Hub table Status column provides a quick view of the health of the event hub. The meaning of the status colors is as follows:

- Green: Good. The Comments column reads All Good.
- Blue: Not yet configured.
- Gray: Unavailable.
- Orange: Warning.
- Red: An error condition. The Comments column might contain useful information about why the error occurred.

Tip: Hover your mouse over a status spot to see a status description.

## Enable and disable monitoring

---

From the Event Hubs header, you can enable or disable monitoring for individual event hubs.

- To start monitoring an event hub, select a disabled event hub and click Enable Monitoring.
- To stop monitoring an event hub, select a running event hub and click Disable Monitoring.

## View information about individual collectors

---

For central manager configurations: When an event hub is enabled, the Event Hub column displays a small  icon. Click the  to show details about each collector. In the Monitor enabled column, you can turn individual collectors on and off.

## View status history

---

Select an event hub and then click Status History to view the status history for this event hub. The following information displays for each collector in the event hub:

- Status from and Status to: The start and end times for this status history period. When the state changes, the status history period ends.
- Collector (for central manager configurations): The collector for this status history period.
- Status: The state of the collector during this period.
- Comments: Notes about the status. When a collector fails, the Comments section often contains useful information about why the failure occurred.

## Filter event hub data

---

From the Event Hubs header, enter text into the Filter dialog. The Event hubs table displays any stream with text that matches the filter text; the remaining event hubs are hidden.

---

## Cloud database service protection with native audit

Cloud database protection provides classification, vulnerability assessment, and object auditing on cloud databases, using the native audit.

After you set up the Guardium® connection with the cloud, you can:

- Discover database instances, and catalog them in Guardium.
- Assign catalogued data sources to a Classification process or create a new process: Classification runs on the cloud databases and identifies objects according to the defined rules.
- Assign catalogued data sources to a Vulnerability Assessment (VA) process or create a new process (requires a valid VA license): VA runs on the cloud databases and uses the data in Guardium reports.
- Enable DB auditing: Oracle Standard Auditing data is pulled from the cloud for Guardium reports, depending on installed policies. For more information, see the Oracle documentation about Database Auditing.
- Enable object auditing (Oracle's audit trail):

- Review the Classification results and select objects for object auditing. (DB auditing must be enabled.) Object auditing tracks all activities that are performed on the objects. Guardium uses this data in reports, the investigation dashboard, and other areas.
- Configure Guardium to add objects automatically, per data source.
- Set a default per account, inherited by all of its data sources. Setting a default is especially useful for databases whose objects need auditing without any further evaluation. Set a high but reasonable limit of what you expect the classification process to find. You also want to prevent an overflow of objects if there is a mistake in your classification, so don't set it too high. (An overflow can affect the database performance.)

Note: AWS permissions are required to perform Guardium functions on the cloud DB. See [Define AWS IAM for native audit](#).

In on-premises databases, the S-TAP installed in the database sends all database traffic to the Guardium system. In the cloud environment, Guardium pulls log files from the cloud DB, and processes the data similar to S-TAP data. The difference is that the S-TAP records all database activity, whereas in the cloud environment, only the tables that you select are audited. Another difference is that there can be a slight delay in data retrieval from the cloud.

Activity on audited databases and objects is written to the database logs. The volume of log activity increases with the number of monitored items. High volume log activity can impact the database performance. You need to ensure that you are capturing all relevant data, while not overloading the system.

You can run cloud database service protection in a central manager environment and on a stand-alone Guardium collector.

In the context of cloud DB service protection, database refers to the database on the cloud, and data source refers to the Guardium cataloged database.

Only one Guardium system can own the DB audit and object audit of any one DB. Other Guardium systems can access the same cloud account and see the DB details, but cannot disable the DB audit or access the object audit data. You can move ownership from one Guardium system to another, for example if one goes down without expectation of recovery.

Discovery, Classification, and VA are supported for all Amazon RDS database engines.

**Limitations:**

- You must keep the RDS definition updated, for example, DB instance deletions, or changes in credentials.
- Guardium supports Oracle V.11, V.12, V.18, V.19 databases on an AWS cloud. (Since Oracle 12 audit does not contain login records, the client IP is not available.)
- Extrusion rules are not supported, including redaction and testing for patterns in the returned data.
- Return data is not supported, including records affected and logging of bind variable values.
- Rule actions that interact with S-TAP are not supported; for example, S-GATE Terminate, Ignore, and query rewrite.
- Failed logins are not captured by the Oracle audit, and therefore are not forwarded to Guardium.
- Statements not captured by the Oracle audit, for example Statements with syntax errors, cannot be monitored.
- Audit data has bind variable values but not type, for example, 123, so when it is replaced in SQL, surrounding quotation marks are always added.
- When variable values contain ASCII control character, for example, '\001' or multiple byte characters, the audit file is not downloadable.
- Blob bind variable values are not supported.
- [Cloud database service protection workflow](#)  
Provide protection for your cloud database services by using native audit.
- [Define AWS IAM for native audit](#)  
Define the Identity and Access Management (IAM) policy for your Amazon Web Services (AWS) account, depending on the required permissions.
- [Create, modify, delete cloud accounts](#)  
Create a Guardium cloud DB service account with your database credentials, and modify or delete the cloud account.
- [Discover cloud databases](#)  
Discover databases in the cloud account by selecting the regions you want to search.
- [Catalog and manage databases](#)  
Catalog databases to create the datasources in Guardium, modify users and passwords, and update the database configuration.
- [Manage Classification and Vulnerability Assessment](#)  
Assign datasources to an existing classification or vulnerability assessment process, or create new processes.
- [Configure database auditing](#)  
Enable auditing on the database so that object auditing data can get pulled by Guardium. Modify the limit of objects added automatically to classification, and modify the collector.
- [Manage object auditing](#)  
View the potentially sensitive objects identified by the classification processes in the databases that you manage, and enable object auditing on selected objects to monitor all activities performed on these objects.

## Cloud database service protection workflow

Provide protection for your cloud database services by using native audit.

### About this task

This is a general workflow for providing cloud database service protection with native audit. Your specific workflow depends on what you want to achieve with the cloud database audit.

### Procedure

1. Define the AWS Identity and Access Management policy as described in [Define AWS IAM for native audit](#).
2. Create a cloud account as described in [Create, modify, delete cloud accounts](#).
3. Discover its database instances as described in [Discover cloud databases](#).
4. Catalog the databases that you want to work with as described in [Catalog and manage databases](#). Cataloging creates a data source within Guardium so that you can manage the cloud database Guardium functions on the specific database.
5. Optionally add the data source to a new or existing VA process (requires Vulnerability Assessment license) or to a new or existing Classification process. For more information, [Manage Classification and Vulnerability Assessment](#).
6. Optionally enable DB Audit on relevant databases, as described in [Configure database auditing](#). Restart the databases either now from the Guardium UI, or later from the DB console. After DB auditing is enabled, it performs standard Oracle auditing. When you enable DB Auditing, your Guardium system becomes the unique

- owner of the DB Audit on this DB. No other Guardium system can modify the DB Audit or the object audit. To see Classification results, run Classification once (Run once now) after you enable the DB Audit, or wait for the next scheduled run. (The data source must be assigned to a Classification process.)
7. Review the Classification results of your data sources (requires a classification process and DB Audit):
    - View the objects, grouped either by the object or the classification process that identified the objects, and use filters to further refine the results
    - Enable or disable object audit: individually, by table
    - Drill down from the objects grouping to open a list of all databases that contain the selected object in their classification results. In this view, you can also enable and disable object auditing.
  8. Periodically repeat steps [3](#) through [7](#).
  9. Review the data sources periodically, checking for New objects, and optionally adding or removing objects from the object audit. For example, you might remove objects that do not need auditing but were automatically added, or if a database is having performance issues. Or you might identify a suspicious object that is not audited, and add it to the object audit.

## Define AWS IAM for native audit

Define the Identity and Access Management (IAM) policy for your Amazon Web Services (AWS) account, depending on the required permissions.

### Minimum permissions

The minimum IAM permissions include viewing configuration and changing tags. They do not include enabling the DB audit, or restarting a DB. The following JSON example defines the minimum permissions, without which you cannot run cloud database service protection.

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Action": [
 "rds:DescribeDBParameters",
 "rds:DescribeDBInstances",
 "rds:DescribeDBParameterGroups",
 "rds:DownloadDBLogFilePortion",
 "rds:DescribeDBLogFiles",
 "rds>ListTagsForResource",
 "rds:RemoveTagsFromResource",
 "rds:AddTagsToResource",
 "ec2:DescribeSecurityGroups",
 "ec2:DescribeVpcs"
],
 "Effect": "Allow",
 "Resource": "*"
 }
]
}
```

### Additional permissions

Full permission is enabled with these parameters.

Enable, disable DB audit on instance

When not configured, the Enable DB Auditing and Disable DB Auditing buttons are disabled. You need to ask your DBA to enable or disable the DB instance on the AWS console.

```
"rds:CopyDBParameterGroup",
"rds>CreateDBParameterGroup",
"rds:ModifyDBInstance",
"rds:ModifyDBParameterGroup",
```

Restart DB instance

When not configured, Restart is disabled, and you need to request the DBA to restart the DB instance on the AWS console.

```
"rds:RebootDBInstance",
```

Handle security group when the supported platform is EC2

When not configured, the DBA needs to add the Guardium® IP to the security group. When configured, Guardium adds its IP to the security group of the DB instance. If the Guardium system cannot identify its own IP due to the network configuration, then the DBA needs to add the IP on the AWS console.

```
"rds:ModifyDBInstance",
"rds:AuthorizeDBSecurityGroupIngress",
"rds>CreateDBSecurityGroup",
```

Handle security group when the supported platform is VPC

When not configured, the DBA needs to add the Guardium IP to the security group. When configured, Guardium adds its IP to the security group of the DB instance. If the Guardium system cannot identify its own IP due to the network configuration, then the DBA needs to add the IP on the AWS console.

```
"rds:ModifyDBInstance",
"ec2:AuthorizeSecurityGroupIngress",
"ec2>CreateSecurityGroup",
```

When configuring these parameters, Guardium creates an inbound rule in the RDS instance security group, with collector public IP CIDR mask = 24.

## Create, modify, delete cloud accounts

Create a Guardium cloud DB service account with your database credentials, and modify or delete the cloud account.

## Create cloud account

---

### About this task

Create cloud accounts to manage the connection between your cloud databases and Guardium®.

Tip: If you are managing multiple databases in this account, consider defining a default classification process so that you do not need to define the properties for each discovered database.

### Procedure

1. Browse to Discover > Database Discovery > Cloud DB Service Protection.
2. Click  to open the Create Cloud DB Service Account Definition pane.
3. Define the account:
  - Name: An account name that is unique to your site.
  - Provider: Select the provider name from the menu. Currently Amazon is the only available provider.
  - Audit type: Select Native.
  - AWS access key ID and AWS secret access key ID: Supplied by your cloud services provider. The account secret key functions as a password. Make sure that the access key and title are both unique so that you do not have multiple account names with the same access\_id.
4. Configure Database Auditing and Classification:
  - Default classification Process. Optional. All cataloged databases in this account are assigned to the specified classification process. You can modify the classification process, per database, after they are cataloged.
  - Limit objects added automatically: When the DB Auditing is enabled, you can specify the maximum number of objects that are found by classification to automatically enable for object auditing. You can modify the number of objects to find, per database, after they are discovered. Objects that are enabled automatically appear as Enabled in the managed objects window. To add objects automatically, set a high but reasonable limit of what you expect the classification process to find. To prevent an overflow of objects if there is an error in your classification, don't set the limit too high (which can affect the database performance). Let's say that you set the limit to 15, and classification identifies five objects on the first run. Those five objects are enabled for DB Audit. The next classification run identifies five more objects, and those objects are also enabled. However, no new objects are enabled if the number of audited objects plus the number of newly classified objects exceeds the specified limit. Therefore, if the next Classification run identifies seven objects, then those objects are not enabled, because that will exceed the specified limit (15). If set to zero, objects are not automatically enabled for object auditing.
5. Test access to the cloud. Click Test Access to make sure that your account has access to the cloud.  
If the test fails to access the cloud, check the following items:
  - Your Guardium system has access to Amazon.
  - You supplied the correct keys.
6. Click Create.  
The account is created and the Cloud DB Service Accounts list updates with the new Cloud account.

### What to do next

Discover databases and catalog them, set up classification and vulnerability assessment, and object auditing. For more information, see [Discover cloud databases](#).

## Modify a cloud account

---

You can modify all parameters except the provider.

### Procedure

1. Select the cloud account under Cloud DB Service Accounts, and click  in the right pane.
2. Modify the configuration.
3. If you modify any credentials, click Test Access to test the access to the cloud.
4. Click Save.

## Delete a cloud account

---

For data streams, deleting an account disconnects the database from the Guardium managed units. For native audit, deleting an account disables the object audit and the DB audit on all the databases owned by the current environment.

### Procedure

1. Select the account in the Cloud DB Service Accounts pane, click , and confirm.
2. Restart the DB from the DB console. If you do not have Amazon access to the DB, ask your DBA to disable DB auditing and to restart the DB. It's important to stop auditing and restart the DB so that the DB stops writing to the Guardium log files.

## Discover cloud databases

---

Discover databases in the cloud account by selecting the regions you want to search.

### About this task

---

The databases table is populated and updated when you run Discover. Once a database has been discovered, it stays in the table, regardless of whether the database is still in the cloud..

Every time you navigate to Discovery > Database Discovery > Cloud DB Service Protection, Guardium informs you if the DB auditing status in the cloud is different from the status reported in the UI, with a message above the Database table: DB auditing status has changed for some databases. Click Refresh to update the table. When you see this message, click Refresh to refresh the display.

You can also perform this check on demand by clicking Retrieve status. The retrieve can take a few minutes. When it's complete, a message appears only if any of the DB audit statuses have changed. If there are changes, click Refresh.

You can also upload cloud database definitions by CSV file. The required parameters are listed in [Cloud Datasource APIs](#); the API parameter **cloudTitle** must be replaced with the parameter **environmentTitle** (they have the same function, but different names). See the upload procedure in Create Datasource for CSV uploaded via the Upload CSV menu in [Customer Uploads](#), using the path Harden > Vulnerability Assessment > Customer Uploads to upload your file.

## Procedure

---

1. Navigate to Discovery > Database Discovery > Cloud DB Service Protection, and click the service account name.  
When you create a cloud account, the Discover Databases table is open, showing a list of all of the regions, with their RDS endpoints.
2. When you access this page subsequently, the table is closed. Click Discover Databases.  
The table opens showing the regions.
3. Select the row of each region whose databases you want to discover. Use the filter if relevant.
4. Click Discover.  
Guardium searches the regions, and adds any databases that were not previously discovered to the databases table.

## Catalog and manage databases

---

Catalog databases to create the datasources in Guardium, modify users and passwords, and update the database configuration.

### About this task

---

Cataloging creates the datasources within Guardium® that are used for classification, vulnerability assessment, auditing, and reports. Databases that are not cataloged have a red icon in the GuardiumDatasource column of the DB table.

## Procedure

---

1. Catalog the databases you want to audit.
  - a. In the Databases table, select one or more databases.
  - b. Click Datasource > Catalog Datasource.
  - c. Enter the case-sensitive DB user and password that you received from your DBA. If you selected more than one database, be sure you want them to use the same user and password pair.
  - d. Optionally select, modify or clear the default Classification process.
  - e. Click Catalog.The Guardium datasource name appears in the Databases table.
2. Update the user or password:
  - a. In the Databases table, select one or more datasources.
  - b. Click Datasource > Update User and Password and modify the details. Both fields must be specified.
  - c. Click Catalog.
3. Modify one datasource definition.
  - a. Select the datasource and click Datasource > Open Datasource Definition
  - b. Modify as relevant. See parameter details in [Creating a datasource definition](#).
  - c. Optionally test connectivity to the database by clicking Test Connection.
  - d. Click Save.

## Manage Classification and Vulnerability Assessment

---

Assign datasources to an existing classification or vulnerability assessment process, or create new processes.

### About this task

---

The Vulnerability Assessment menu is available only if you have a valid VA license.

Once you assign a classification process to a datasource, classification data is collected and handled the same as an on-premises database. You can assign classification when you are not the owner, but you must take ownership in order to enable object audit and view the results.

A green icon indicates the process is running. A yellow icon means there is no schedule defined for the process. A red icon in the Classification Process or VA column indicates no classification or VA assigned, or an error. View VA errors in Harden > Vulnerability Assessment > Assessment Builder > View Results. View classification errors in Discover > Classification > Discover Sensitive Data > Review Report ribbon > Process Log.

If you get a classification error `file bdump-file-listing in BDUMP not found Unable to retrieve results for: 'RDSADMIN.TRACEFILE'` add RDSADMIN to the pre-defined schema group Excluded Classification schemas - Oracle in the Group Builder.

## Procedure

---

1. Assign one or more datasources to an existing Classification process.

- a. Select one or more datasources.
  - b. Click Classification > Add to Classification.
  - c. Select the Classification Process and click Save.
  - d. Optionally click Edit/View to modify or run the classification process.
  - e. If you want to enable object auditing automatically for the objects found by classification process, click **Edit/View** to open the classification process; in the Where to search ribbon, select the checkbox Enable object auditing for Cloud DBs.
  - f. Alternatively, run the classification: click Run Now in the Run Discovery ribbon in the Discover > Classification > Discover Sensitive Data.
2. Create a new Classification process, and assign one or more datasources to it.
    - a. Select one or more datasources.
    - b. Click Classification > Create Classification.
    - c. Follow procedure in [Discover Sensitive Data](#). Enable object auditing for Cloud DBs is selected by default. Leave it selected.
    - d. Run the classification: after you define Where to Search, click Run Now, or after you save the process click Run Now in the Run Discovery ribbon.
  3. Assign one or more datasources to an existing Vulnerability Assessment.
    - a. Select one or more datasources.
    - b. Click Vulnerability Assessment > Add to Vulnerability Assessment.
    - c. Select the Vulnerability Assessment process and click Save.
    - d. Run the process: navigate to Harden > Vulnerability Assessment > Assessment Builder, select the process and click Run once now.
  4. Create a new Vulnerability Assessment, and assign one or more datasources to it.
    - a. Select one or more datasources.
    - b. Click Vulnerability Assessment > Create Vulnerability Assessment.
    - c. Enter a description of the vulnerability assessment; enter one or more email addresses, separated by commas, to receive the results as part of an audit process that you define.
    - d. Click Save.

The VA process is created with all tests, the selected datasources, and the receivers you defined.

    - e. Run the process: navigate to Harden > Vulnerability Assessment > Assessment Builder, select the process and click Run once now.

## Configure database auditing

Enable auditing on the database so that object auditing data can get pulled by Guardium®. Modify the limit of objects added automatically to classification, and modify the collector.

### About this task

The databases table presents various details of the discovered databases. You can use the colored indicators in the table to see the status of any datasource at a quick glance. Red indicates no configuration, for example the database is not cataloged, or the datasource was not assigned to a classification or VA process. There are hover tips on the color-coded status indicators to give you more information when the color is red or yellow. Use the predefined filter list to filter any of the columns that have the color-coded status indicators, or the free text filter for other values.

If there is a collector defined for the datasource, it appears in the Active Collector column if you are the owner. Otherwise the column is blank.

The DB Audit Owner is the CM host name in a CM environment. In a standalone system the value is the collector's host name.

The DB Auditing column has one of the following values.

- Enabled. When followed by pending restart, indicates that the status will take effect upon instance restart.
- Disabled. When followed by pending restart, indicates that the status will take effect upon instance restart.
- configuration does not match requirement. (The AWS parameter audit trail is not configured according to Guardium's requirement XML, EXTENDED. Ask your DBA to modify this value.) When followed by pending restart, indicates that the status will take effect upon instance restart.
- Not supported for this db engine. Activity monitoring is not currently supported by Guardium.

If you own the instance, a classification process is assigned, and DB audit is enabled, you should see results in the Objects column. The total is the number of objects identified by the classification processes assigned to this instance; Audited is the number of those objects that are enabled for Object Audit; New is the number of objects that have been found by a classification process but have not been enabled automatically. These objects require review. See [Manage object auditing](#).

You should see results in the Objects column if the datasource is assigned to a classification process, the process has run since enabling the DB audit, and you are the owner. If you don't see objects, verify the classification process and run it again.

## Modify limit of objects added automatically and collector

You can modify the limit of objects added automatically and the collector on one or more databases simultaneously. Fields that are left blank are not modified.

### Procedure

1. Select one or more databases.
2. Click DB Auditing > DB Auditing Configuration .
3. Modify the number of Limit objects added automatically. When the DB Auditing is enabled, you can specify the maximum number of objects that are found by classification to automatically enable for object auditing. You can modify the number of objects to find, per database, after they are discovered. Objects that are enabled automatically appear as Enabled in the managed objects window. To add objects automatically, set a high but reasonable limit of what you expect the classification process to find. To prevent an overflow of objects if there is an error in your classification, don't set the limit too high (which can affect the database performance). Let's say that you set the limit to 15, and classification identifies five objects on the first run. Those five objects are enabled for DB Audit. The next classification run identifies five more objects, and those objects are also enabled. However, no new objects are enabled if the number of audited objects plus the number of newly classified objects exceeds the specified limit. Therefore, if the next Classification run identifies seven objects, then those objects are not enabled, because that will exceed the specified limit (15). If set to zero, objects are not automatically enabled for object auditing.
4. Collector appears in, and is mandatory for, a Central Manager environment. Select a collector from the drop-down list of all collectors in the CM environment. This is the collector that pulls the audit data (activities) from the DB.
5. Click Apply.

## Enable auditing on one database

---

You can enable DB auditing on one database at a time.

### About this task

You can configure the parameter Limit objects added automatically or the collector with any permission level. Other changes require DB permissions. Your access keys may or may not include these permissions. The instructions below cover all levels of permission.

When you enable DB Auditing, your Guardium system becomes the unique owner of the DB Audit on this DB. No other Guardium system modify the DB Audit or the object audit. Another system can forcefully take ownership by clicking Start owning DB Audit.

Run classification at least once after enabling DB audit to see and manage objects for auditing. If no objects are found, check your policies.

#### CAUTION:

When you start managing the database, the Amazon RDS tag IBM Guardium IP is created with the value of your Guardium hostname. This tag should not be modified or removed.

### Procedure

1. Select the row of the database.
2. Click DB Auditing > DB Auditing Configuration.
3. Optionally modify the value of objects added automatically to the Object Audit.
4. In CM environment, if there is no collector defined, select one from the drop-down list and click Apply. The dialog refreshes, and the buttons are enabled.
5. If Enable DB Auditing is enabled, click it. The dialog and the table refreshes showing You are now owner of the DB audit. The dialog box refreshes. Either click Restart to restart the database now (a confirmation message appears), or click Wait for next manual restart for example, to wait for a maintenance window. If you choose Wait for next manual restart, you need to access the cloud console directly at a later time. If you click Restart and you do not have sufficient access rights, an error appears. Request your DBA to configure **audit trail** as XML, EXTENDED and restart the instance.
6. If Enable DB Auditing is not enabled, click Own DB Audit. The dialog box refreshes. Click Wait for next manual restart and request your DBA to configure **audit trail** as XML, EXTENDED and restart the instance.
7. If you made changes to the DB audit status, click Retrieve Status and wait for the message saying the status has changed, then click Refresh. The DB Audit Owner column shows the host name of the CM or the collector's hostname in a standalone Guardium, and the icon in the DB Auditing turns green.

## Disable auditing on one database

---

You can disable DB auditing on one database at a time. When you disable the DB audit, you also relinquish ownership of the DB auditing.

### About this task

When you stop owning or disable the DB Audit, the entire object audit is disabled as well and the list of objects that can be audited (the come from the classification results) are deleted.

### Procedure

1. Select the row of the database.
2. Click DB Auditing > DB Auditing Configuration.
3. Click Disable DB Auditing, then click Wait for next manual restart, for example to wait for a maintenance window, or click Restart to restart the database now. If you choose Wait for next manual restart, you need to access the cloud console directly at a later time. If don't have permission to change the configuration, click Stop Owning DB Audit and request your DBA to disable the DB audit on this instance.
4. Click Retrieve Status to refresh the display with the latest status from the cloud.

### Results

If there were changes, a message appears: DB auditing status has changed for some databases. Click Refresh to update the table. Click Refresh. The status changes to disabled or disabled pending restart, the icon in the DB Auditing turns red, and the DB Audit Owner column is blank.

## Starting and stopping DB audit ownership

---

### About this task

You can modify the DB ownership status of one database at a time.

Owning the DB Audit gives you exclusive rights to the DB Audit and Object Audit definitions, and access to the object audit data (see [Manage object auditing](#)). Other Guardium systems can access the same cloud account but can only see the DB details.

With full access rights, when you enable the DB audit, you also take ownership of the DB. If your access keys do not provide full access rights, then you take ownership without enabling the DB audit. When DB audit is enabled (by the DBA) you will have access to the audit data. Conversely, when you disable the DB Audit, you relinquish ownership. If your access keys do not provide full rights, you would stop owning DB audit, and request the DBA to disable the DB audit.

You can move ownership from one Guardium system to another.

If you are transferring ownership between two live systems, first stop owning the DB Audit on the current owner, then take ownership on the second Guardium system. All auditing is stopped when one Guardium system relinquishes ownership. You'll need to define the auditing process on the new Guardium system: assign the DB to a classification, run the process, and add objects to the Object Audit.

#### CAUTION:

Stop owning the DB Audit on one before starting to own it on the second. Otherwise the data will go to the previous collector, as well as the new collector. Two collectors with different policies (different CMs) receiving the same activities, produce different, or incomplete, results on each collector.

If you are transferring ownership from a Guardium system that has gone down without expectation of recovery, you can start owning the DB Audit from another Guardium system, while maintaining the audit definitions, only the ownership changes. In this scenario, stop the original Guardium from owning the DB Audit in the DB console.

### Procedure

1. In the databases table, select the row of the database.
2. To stop owning DB audit: Click DB Auditing > DB Auditing Configuration > Stop owning DB audit.
3. To start owning DB audit: Click DB Auditing > DB Auditing Configuration > Start owning DB audit.

## Manage object auditing

View the potentially sensitive objects identified by the classification processes in the databases that you manage, and enable object auditing on selected objects to monitor all activities performed on these objects.

### About this task

**Prerequisite:** DB auditing must be enabled and owned by you, and classification must run at least once on this the datasource.

New objects are objects that have been found by classification processes that have not been enabled for auditing. You can filter for all new objects, and then either enable them for object auditing, or clear the **New** flag. When there are no New objects, then you are up to date with evaluating the new objects. Remember, Guardium® could receive new data every time the classification process runs. When new objects are found that were not added automatically to the object audit, there is a notice **New objects were found**.

The **Found by Classification** column lists all the classification processes that identified this object.

The status Mixed in the Object Audit Status column means the object audit is enabled in some datasources and disabled in other datasources.

Enabling and disabling object auditing is a heavy process, and can take a few minutes. There is a waiting icon while the cloud processes the auditing changes.

You can review objects found in one datasource or multiple datasources by selecting the rows of the datasources you want to review from the Databases table. The object audit windows shows all objects found by all classification processes on the selected database or databases.

- [Managing object audit in one database](#)
- [Managing object audit in multiple databases](#)

## Managing object audit in one database

### About this task

The Objects in Datasource <name> window lists all objects found by the classification processes run on this datasource. Objects can be found by more than one classification process.

When objects have been identified by the classification process but were not enabled automatically for object audit, **New objects found** appears above the objects table. Click New Only to filter for all new found objects that require handling. New objects could be found every time the classification runs. When there are no New objects, you are up to date with the new objects evaluation.

Review the data sources periodically, checking for New objects, and optionally adding or removing objects from the object audit. For example, you might remove objects that do not need auditing but were automatically added, or if a database is having performance issues. Or you might identify a suspicious object that is not audited, and add it to the object audit.

Use the classification filter for objects that you know must be audited. Select all objects in the filtered view, and enable object auditing.

### Procedure

1. If you assigned the Classification process **before** you enabled DB Audit, run the Classification once now and wait a few minutes (or wait for the next scheduled run) for Guardium® to identify objects.
2. Select one datasource. Consider using the filter New objects found to identify datasources with new objects.
3. Select DB Auditing > Manage Object Auditing.  
The Manage Object Auditing window opens listing all objects found by the classification processes to which this datasource is assigned.
4. Consider using the filter New only to identify all objects classified as New.
5. Select one or more objects (rows) in the table.
6. To enable audit trail, select Actions > Enable Audit.  
The system responds with the success or failure of the operation.
7. To clear the New flag, click Actions > Clear New flag.
8. To disable audit trail, select Actions > Disable audit.  
The system responds with the success or failure of the operation.

## Managing object audit in multiple databases

### About this task

This view lists all objects found by the classification processes run on the selected datasources. Objects can be found by more than one classification process. View the objects grouped by object (default), or classification. The Found by Classification column lists all the classification processes that identified the object.

When objects are identified by the classification process but were not enabled automatically for object audit, **New objects found** appears above the objects table. Click New Only to filter for all new found objects that require handling. Review the New objects and either enable object auditing, or clear the New flag.

New objects could be found every time the classification runs. When there are no New objects, you are up to date with the new objects evaluation.

Review the data sources periodically, checking for New objects, and optionally adding or removing objects from the object audit. For example, you might remove objects that do not need auditing but were automatically added, or if a database is having performance issues. Or you might identify a suspicious object that is not audited, and add it to the object audit.

**Group by Object:** To view all new found objects, type New in the text filter.

To enable or disable the object audit on one object in all the selected datasources, select the row(s) and click Action > Enable / Disable

To take action per datasource, click Present in # datasources to view all datasources whose classification processes have identified the selected object

**Group by Classification** is especially useful when you have almost identical datasources, or classification policies, whose objects need auditing without any further evaluation, for example GDPR.

## Procedure

1. If you assigned the Classification process **before** you enabled DB Audit, run the Classification once now (or wait for next scheduled run) and wait a few minutes for Guardium® to identify objects.
2. When grouped by object:
  - a. Select multiple datasources that have New objects in the Objects column of the Databases Table. Use the filter New objects found to identify these datasources.
  - b. Click DB Auditing > Manage Object Auditing. The Manage Object Auditing window opens.
  - c. If the object must always be audited in all the datasources, select the row(s) and click Actions > Enable Audit.  
The system responds with the success or failure of the operation.
  - d. If you want to enable the object audit on individual databases, click the number in the Present in # Datasources column, in the row of the object to open the Datasources containing <object> window. This window shows all datasources whose classification processes have identified the selected object. Select one or more datasource rows and click Actions > Enable Audit.
3. For a classification process whose identified objects always need auditing without further evaluation: Click the Classification radio button (above the table); select one or more rows of classification processes, and click Actions > Enable Audit.

## Database discovered instances rules

Use the Database Discovered Instances Rules UI from a central manager to determine how to manage inspection engines for discovered databases.

### Before you begin

Before you configure the Database Discovered Instances Rules in the GUI, you need to enable inspection engine creation by using the `modify_guard_param` API command from the CLI. To enable creating inspection engines, call the following API:

```
grdap! modify_guard_param paramName=IE_CREATION paramValue=1
```

For more information, see the [modify\\_guard\\_param](#) API command.

### Configuring the database discovered instance rules

Guardium® can be configured to discover databases that are created on both Windows and UNIX systems. In many cases, you might want Guardium to create and run inspection engines on all newly discovered databases. However, there are scenarios in which you want control when and how Guardium creates new inspection engines. In these cases, Database Discovered Instances Rules provides a way to manage inspection engine creation. You can configure discovered instances rules from a central manager in a managed environment or on a stand-alone system.

From a central manager, select Database Discovered Instances Rules from Discover > Database Discovery .

From the GUI, you can take the following actions:

- Click Enable to start automatically creating inspection engines.
- 12.1 and later Click Manage Collectors to view a list of collectors that are managed by the central manager. You can filter the collectors by status and use the check box to quickly and easily enable or disable multiple collectors.
- To generate a report of the discovered instances rules without creating inspection engines, select the Report results of discovered instances rules (don't create inspection engines) checkbox. You can use this report to:
  - Determine the impact of your changes before you create new inspection engines.
  - Report on changes to your existing database configurations (such as unexpected changes to port ranges or [for UNIX] DB installation directory).
- Select whether you want to manage inspection engines for a Windows or UNIX environment.
- Choose whether to create inspection engines for all discovered databases, or to specify rules that determine when an inspection engine is created.

If you select Specify rules to create inspection engines, then you can specify rules for your site.

Note: By default, if parameters for an existing inspection engine are a 100% match with an inspection engine that matches a newly discovered database, Guardium does not create a new inspection engine.

## Creating inspection engines use cases

Table 1. Inspection engine use cases

| Rule | Existing inspection engine | Newly discovered instance |  | Use case |
|------|----------------------------|---------------------------|--|----------|
|      |                            |                           |  |          |

| Rule    | Existing inspection engine              | Newly discovered instance                    | Use case                                                                                                                                                                                                                                                 |
|---------|-----------------------------------------|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Filter  | Ignore                                  | Add or ignore, depending on filter criteria. | You want to detect only inspection engines that meet certain criteria, such as specified ports, protocols, or servers. Create a filter to prevent creating inspection engines that do not meet the criteria.                                             |
| Exclude | Remove                                  | Don't add inspection engine.                 | You have database instances that no longer need monitoring. Delete existing inspection engines that meet the rules, and do not add an inspection engine if it meets the specified rules. Use an advanced rule to specify a rule that requires operators. |
| Ignore  | Keep                                    | Don't add inspection engine.                 | You have inspection engines that you want to keep, regardless of whether they are discoverable (such as a late mount configurations or a passive cluster). Preserve existing configurations that meet all of specified rules.                            |
| Replace | Remove                                  | Add                                          | Update existing inspection engines to meet new criteria, such as upgrading to a new database version or changing the installation directory path.                                                                                                        |
| Merge   | Update or remove, depending on settings | Ignore, depending on settings                | Consolidate existing inspection engines and discovered instances to avoid creating new and unnecessary inspection engines.                                                                                                                               |
| Add     | Keep                                    | Add                                          | Create an inspection engine whenever a new database is found in your environment and the newly discovered instance does not match any of the Filter, Exclude, Ignore, or Replace rules.                                                                  |

## Specifying inspection engine rules

The rules to create inspection engines fall into the following categories: Filter, Exclude, Ignore, Replace, and Add. The rules are hierarchical. That is, Guardium checks the Filter rule first; if it does not apply, then it checks the Exclude rule, and so on. If none of the rules applies, Guardium creates (adds) a new inspection engine.

Note: For all rules, click the Add rule  to add an OR statement. Click the  after the parameter to add an AND statement.

To define rules:

1. Click Filter to open the Filter pane. Use Filter to specify ports, protocols, or servers to ignore (that is, to filter out those inspection engines from discovery).
  - a. Click Add rule to add a filtering rule.
  - b. Select a parameter from the parameter list and specify a value for that parameter.

Note: For the Port range start and Port range end parameters, if you select the in or not in operators, separate multiple values with commas, and use a hyphen to specify an inclusive range of ports. For example: 1520-1530, 1621, 1622.

2. Click Exclude to open the Exclude pane. Use Exclude to delete outdated inspection engines.
  - a. Click Add rule to add an exclude rule.
  - b. Select a parameter from the parameter list and specify a value for that parameter.

Important: If any of the specified parameters match inspection engine parameters, Guardium deletes that inspection engine. Therefore, you need to be precise about which parameters you select.

For example, if you specify only the Exclude rule DB version = 12, Guardium deletes the inspection engines on any database type with version 12 (such as Oracle 12c, Informix® v12.10, or Db2® v12).

3. Click Ignore to open the Ignore pane. Use Ignore to determine whether an inspection engine exists that meets all of the match criteria. If an exact match is found, Guardium does not create a new inspection engine (that is, Guardium ignores the new database instance).

Note: A built-in implicit Ignore rule checks new discovered database instances against all of the available criteria. When all criteria match, the Ignore rule is triggered. Therefore, in general, you do not need to configure this rule.

4. Click Replace to open the Replace pane. Use Replace to update individual parameters in one or more inspection engines. Guardium provides suggested match criteria for Replace, but these are not required.

For example, say that your site updates the database version and installation directory for a database. In this case, you want to update only the DB version and DB install dir parameters for the existing inspection engines. To do so, specify all of the parameters for the inspection engines to match against; that is, everything except DB version and DB install dir. Guardium compares all of the newly discovered databases (with the new database version and installation directory) against all of the inspection engines and updates the inspection engines that match the selected criteria. Since you did not specify the DB version and DB install dir, the corresponding inspection engines are updated with the new version and install directory parameters.

5. Click Merge to open the Merge pane. The following merge options provide ways of associating discovered instances with existing inspection engines to avoid creating new and unnecessary inspection engines:

Do not create inspection engine for discovered instances where port range is within matching inspection engine port range

Enabling this setting reuses inspection engines when the port range of a discovered instance is within the port range of an existing inspection engine. This setting causes Guardium to ignore discovered instances when they meet the following criteria:

- The existing inspection engine port range contains the discovered instance port range
- All of the following criteria match between the existing inspection engine and the discovered instance: db\_type, db\_install\_dir, db\_exec\_file, db\_user, unix\_domain\_socket\_marker

Update inspection engines where port range is within matching discovered instance port range

Enabling this setting expands the port range of an existing inspection engine when its port range is within the port range of a discovered instance. This setting causes Guardium to update the existing inspection engine when the following criteria are met:

- The discovered instance port range contains the existing inspection engine port range
- All of the following criteria match between the existing inspection engine and the discovered instance: db\_type, db\_install\_dir, db\_exec\_file, db\_user, unix\_domain\_socket\_marker

Note: For Oracle databases, if discovery\_ora\_use\_port\_ranges is enabled, this setting allows Guardium to remove redundant inspection engines after the port range of an existing inspection engine is expanded. For more information, see [Discovery parameters](#).

You can further restrict the scope of this setting by defining additional criteria using the  Add update rule (optional) control. The available criteria and operators are the same as what is available for the Filter and advanced Exclude rules.

6. Click Add to open the Add pane. If a newly discovered instance does not meet any of the previous criteria (for Exclude, Replace, or Ignore), Guardium creates a new inspection engine based on the discovered instance.

Note: The Create inspection engines checkbox is selected by default. If you clear Create inspection engines, Guardium does not create inspection engines. In general, make sure that Create inspection engines is selected.

7. When you are done, click Save to save your changes or Cancel to clear all of your changes and start over.

At the Save configuration and overwrite previous settings message, click Save again to save your changes or Cancel to return to your current settings without saving.

The next time Guardium looks for new database instances, the selected rules apply.

## What to do next

---

After you configure the Database Discovered Instances Rules, you can discover database instances from [Manage > Activity Monitoring > S-TAP Control > Send command](#)  to open the S-TAP Commands window.

To run database instance discovery, select Run Database Instance Discovery from the list and then make sure that Replace Inspection Engines is not selected. When you click Apply, database instance discovery runs. For more information, see [Linux-UNIX: Discover database instances](#) or [Windows: Discover database instances](#).

The results of filter rule application details are available in the [Discovered Instances Rules Results](#) report.

You can also add or configure reports and alerts that trigger when an inspection engine changes. For more information, see [Adding reports and alerts for inspection engine changes](#).

Tip: If you encounter an exception when you run the `grdapi apply_rules_on_discoveredinstances` API, make sure that the managed unit is the primary host for the S-TAP. Exceptions can occur when the S-TAP points to multiple appliances and the current managed unit is not set as the primary host.

## Creating inspection engines from the API

---

Use the following APIs to manage inspection engine creation:

- [apply\\_rules\\_on\\_discoveredinstances](#)
- IE\_CREATION, as described under [Inspection engine parameter](#) in [modify\\_guard\\_param](#).
- [Database discovered instance rules scheduler](#)  
Schedule times to search for discovered instances, based on specified rules.
- [Adding reports and alerts for inspection engine changes](#)  
After you configure and enable database discovered instances rules, you can add a report and an alert that triggers whenever an inspection engine is replaced or added.

## Database discovered instance rules scheduler

---

Schedule times to search for discovered instances, based on specified rules.

For managed units and stand-alone systems, use the database discovered instance rules scheduler to specify when you want your system to search for discovered instances, based on the rules you specify for [Database discovered instances rules](#). To open the scheduler, browse to [Discover > Database Discovery > Database Discovered Instance Rules Scheduler](#). For more information, see [Scheduling](#).

Notes:

- From a central manager configuration profile, you can define a schedule for some or all managed units. For more information, see [Working with configuration profiles](#).
- The input for database discovered instances rules comes from S-TAP discovery, which runs on its own schedule. S-TAP discovery typically runs every 24 hours (but you can change it to run more often from S-TAP control). You can see the output of the S-TAP discovery process from the Discovered Instances report on the collector.

## Related concepts

---

- [Scheduling](#)

## Related tasks

---

- [Working with configuration profiles](#)

## Adding reports and alerts for inspection engine changes

---

After you configure and enable database discovered instances rules, you can add a report and an alert that triggers whenever an inspection engine is replaced or added.

## Procedure

---

1. You can access reports in several ways. One method is to browse to My Dashboards and then select either Create New Dashboard or an existing dashboard from your My Custom Dashboards list.
2. From the dashboard, click Add Report and then select Discovered Instances Rules Add or Replace Log.
3. From the Discovered Instances Rules Add or Replace Log report, select  to manage runtime parameters. In addition to the parameters described in [Modifying the runtime parameters](#), you can set the value of Enter Value for Report Only. This option filters data based on the setting (on the Database Discovered Instances Rules page) for Report results of discovered instances rules (don't create inspection engines), as follows,
  - Enter Yes to display only rows where Report results... is selected.

- Enter No to display only rows where Report results... is cleared.
  - Leave the entry as % (the default) to display all rows.
4. By default, alerts generated by Discovered Instances Rules Alert - Discovered Instance Add or Replace are captured in SYSLOG if the alert is active. Use the Alert Builder, as described in [Predefined alerts](#), to modify the alert and select Active to turn on this alert.

## Results

---

When an inspection engine is replaced or added, an alert message is now generated, based on the parameters in the Discovered Instances Rules Add or Replace Log report.

## Classification

Classification policies and processes define how Guardium® discovers and treats sensitive data such as credit card numbers, social security numbers, and personal financial data.

Discovery and classification processes become important as the size of an organization grows and sensitive information like credit card numbers and personal financial data become present in multiple locations, often without the knowledge of the current administrators responsible for that data. This frequently happens in the context of mergers and acquisitions, or when legacy systems have outlasted their original owners. Creating workflows for discovering sensitive data allows you to identify sensitive data in your environment and take appropriate actions, such as applying access policies.

*Classification processes* consist of classification policies that have been associated with one or more datasources. Classification processes can be submitted to be run once or, if login credentials have been stored for all the datasources used in the process, scheduled to run on a periodic basis in a compliance workflow automation process.

*Classification policies* consist of classification rules and classification rule actions designed to find and tag sensitive data in specified datasources.

*Classification rules* use regular expressions, Luhn algorithms, and other criteria to define rules for matching content when applying a classification policy.

*Classification rule actions* specify a set of actions to be taken for each rule in a classification policy. For example, an action might generate an email alert or add an object to a Guardium group. Each time a rule is satisfied, that event is logged, and thus can be reported upon (unless ignore is specified as the action to be taken, in which case there is no logging for that rule).

- [Classification process performance](#)

Classification processes are handled with sampling routines and timeout parameters that ensure minimal performance impact on database servers.

- [Classification Rule Handling](#)

Classification rules are handled according to flexible matching and grouping criteria.

---

## Classification process performance

Classification processes are handled with sampling routines and timeout parameters that ensure minimal performance impact on database servers.

When the classifier runs, you have the option of specifying how it samples records. The default behavior takes a random sampling of rows by using an appropriate statement for the database platform in question. For example, the classifier samples using a `rand()` statement for SQL databases. The alternative behavior is sequential sampling, which reads rows, in order, up to the specified sample size. Random sampling is the default behavior and is recommended because it provides more representative results. However, random sampling may incur a slight performance penalty when compared to sequential sampling.

Attention:

- Random sampling is not supported for Sybase or PostgreSQL: sequential sampling is always used, even in random sampling is selected.
- If random sampling fails on Oracle datasources, sequential sampling is used instead. Random sampling may fail if the classifier encounters certain error conditions, for example selecting ROWID from a join view without a key-preserved table (ORA-1445).
- In some instances, classification rules are applied only to the first 3000 characters, no matter how large or long the sample data is. This 3000 character limitation applies to the following datatypes and datasources,
  - Text data for Sybase and PostgreSQL
  - XML data for MS SQL

For both random and sequential sampling, the default sample size is 2000 rows or the total number of available rows, whichever is fewer. Larger or smaller sample sizes may be specified. If you check the random sampling box, it selects 2000 rows randomly from that table/view and then scans. If the table contains less than 2000 rows, it scans all the rows. If you clear the random sampling box, it selects the first 2000 rows from that table/view and then scans. The default query timeout value is 3 minutes (180 seconds). If the process is running but stuck for 30 minutes, the entire process will be halted.

To further minimize the impact of classification processes on the database server, long-running queries will be canceled, logged, and the remainder of the table skipped. Any rows acquired up to that point will be used while evaluating rules for the table. Similarly, if a classification process runs for an extensive time period without completing, the entire process is halted, logged with the process statistics, and the next classification process is started. This behavior is uncommon and usually only happens on servers that are already experiencing performance problems.

The classifier periodically throttles itself to idle so it does not overwhelm the database server with requests. If many classification rules are sampling data, the load on the database server should remain constant but the process may take additional time to run.

The classifier handles false positives by using excluded groups for schema, table and table columns. Previously, it could be a complex process to set up Guardium to ignore false positive results for future classification scans. Now, when you review classifier results, you can easily add false positive results to an exclusion group, and add that group to the classification policy to ensure those results are ignored in future scans.

---

## Multi-thread classifier

Guardium can run multiple classification threads in parallel to optimize the performance and utilization of the CPU. The number of threads that can run in parallel can be identified by multiplying the number of CPU cores in the machine by 2.

As an example, if there are 4 CPU cores, then 8 would be the maximum number of classifier processes that can be defined and run concurrently. The cap limit, irrespective of the number of CPU cores, is 100.

To retrieve or define the concurrency limit, use [set\\_job\\_process\\_concurrency\\_limit](#).

## Classification Rule Handling

Classification rules are handled according to flexible matching and grouping criteria.

### Fire only with Marker

The Fire only with Marker rule allows for the grouping of Classifier rule types by the same exact name. Additionally, all returned rules using a marker must return data based on the same table name. If two, or more, rules are defined with the same marker then those rules will fire together and together such that if both rules fire on the same table then they both will be logged and their actions invoked. If on the other hand only one of them fires on a table then neither of the rules will be logged or have their actions invoked. Being able to have multiple rules fire together becomes important when you care about sensitive data appearing together within the same table. For example, you may want to know when a table has both a social security number and a Massachusetts drivers license.

Fire only with Marker is a constant value, can be named any value, and must have the exact same value across rules you want to group. This means that if one rule has a marker of ABC then the other rule that you want to group it with must also have a marker named ABC. Any other marker value and the rules are no longer grouped.

You must use at least two rules of any values based on looking for data within the same table name.

### Continue on Match

Fire only with Marker is also based on the Continue on Match rule. As an example, if the following rules are defined such that Rule 3 does not match Continue on Match then no results are returned regardless if all three marker rules were positive. This is because you didn't get to run Rule 4 and the grouping does not fire because all Fire only with Markers must run and return positive results.

Rule 1. Firemarker rule ABC (continue on match)

Rule 2. Firemarker rule ABC (continue on match)

Rule 3. Firemarker rule ABC (continue on match)

Rule 4. Firemarker rule ABC (continue on match)

### Unmatched Columns Only

Use this option for reducing the granularity of data results. Some organizations may want to do a survey of their data to discover which tables and columns have sensitive data without necessarily needing to find every type of sensitive data in that column. A new option for Continue on match, With Unmatched Columns only, means that as soon as the classifier finds a match for that column, it will ignore that column as it continues its processing.

Table 1. Summary of available classifier processing options

| Continue on match | With Unmatched Columns only | Granularity of Result                                                                                                      |
|-------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------|
| No                | N/A                         | Table. Classifier will stop processing rules after the first hit in the table.                                             |
| Yes               | Yes                         | Table and column. Classifier will record the first hit for any given column and ignore it thereafter for subsequent rules. |
| Yes               | No                          | Detailed. Classifier will record hits for all columns for all rules.                                                       |

### Classification with Luhn algorithm

When a rule name begins with guardium://CREDIT\_CARD, and there is a valid credit card number pattern in the Search Expression box, the classification policy will use the Luhn algorithm (a widely-used algorithm for validating identification numbers such as credit card numbers), in addition to standard pattern matching. The Luhn algorithm is an additional check and does not replace the pattern check. A valid credit card number is a string of 16 digits or four sets of four digits, with each set separated by a blank. There is a requirement to have both the guardium://CREDIT\_CARD rule name and a valid [0-9]{16} number in the Search Expression box in order to have the Luhn algorithm involved in this pattern matching.

### Discover Sensitive Data

Create an end-to-end scenario for discovering and classifying sensitive data.

### About this task

Discovery and classification processes become important as the size of an organization grows and sensitive information like credit card numbers and personal financial data propagate to multiple locations. This often happens in the context of mergers and acquisitions or when legacy systems have outlasted their original owners. As a result, sensitive data may exist beyond the knowledge of the person who currently owns that data. This is a common yet extremely vulnerable scenario, since you cannot protect sensitive data unless you know it exists.

Sensitive data discovery scenarios span three critical aspects of enterprise security:

- Discovery: locating the sensitive data that exists anywhere in your environment
- Protection: monitoring and alerting when sensitive data is accessed
- Compliance: creating audit trails for reviewing the results of sensitive data discovery processes

The Discover Sensitive Data end-to-end scenario builder streamlines the processes of discovery, protection, and compliance by integrating several Guardium® tools into a single user-friendly interface.

Table 1. Discover sensitive data tools map

| Value                                                                                      | Scenario Task        | Description                                                                             | Result                                                      |
|--------------------------------------------------------------------------------------------|----------------------|-----------------------------------------------------------------------------------------|-------------------------------------------------------------|
|  Discover | Name and Description | Provide a name and description for the scenario and its related processes and policies. | Creates a classification process and classification policy. |
|                                                                                            | What to discover     | Create rules and rule actions for discovering and classifying data.                     | Optionally creates new datasource definitions.              |
|                                                                                            | Where to search      | Identify datasources to scan.                                                           |                                                             |
|                                                                                            | Run discovery        | Run the scenario.                                                                       |                                                             |
|  Protect  | Review report        | Review the results and define ad hoc grouping and alerting actions.                     | Creates an access policy.                                   |
|  Comply   | Audit                | Define recipients, a distribution sequence, and review options.                         | Creates an audit process.                                   |
|                                                                                            | Schedule             | Create a schedule to run at defined intervals.                                          |                                                             |

This sequence of tasks guides you through the processes of creating a new discovery scenario. This includes creating *classification policies* consisting of rules and rule actions for discovering sensitive data, creating *classification processes* by identifying datasources to scan for sensitive data, defining ad hoc policies (for grouping and alerting, for example), and creating *audit processes* that distribute results to different stakeholders at scheduled intervals.

## What to do next

Continue to the next section and begin creating a discovery and classification scenario.

### 1. [Discovery scenarios](#)

Create a new discovery scenario or select an existing discovery scenario to copy or edit.

### 2. [Name and description](#)

Provide a name and description for your discovery scenario.

### 3. [What to discover](#)

Create policies consisting of rules and rule actions for discovering and classifying sensitive data.

### 4. [Where to search](#)

Identify datasources to scan for sensitive data.

### 5. [Run discovery and review report](#)

Optionally run your discovery scenario and review the results.

### 6. [Audit](#)

Optionally create an audit process by defining receivers, a distribution sequence, and review options for the discovery and classification report.

### 7. [Scheduling](#)

Optionally activate the audit process by scheduling it to run at defined intervals.

---

## Discovery scenarios

Create a new discovery scenario or select an existing discovery scenario to copy or edit.

## Procedure

---

### 1. Navigate to Discover > Classification > Discover Sensitive Data.

### 2. Create, copy, or edit a discovery scenario.

- Click the  icon to create a new scenario.

- Click the  icon to copy an existing scenario or template. When copying a discovery scenario, click the Reuse button to reuse the classification policy associated with the scenario or click the Create copy button to create and use a copy of the classification policy.
- Click an existing scenario name from the Discovery Scenarios list to begin editing that scenario.

Discovery scenarios are displayed in the following format: `scenario`

`name (classification policy name) (datasource type)`. For example, a discovery scenario named `discover_cad1` using the classification policy `policy_cad1` and used with Relational type datasources is displayed as `discover_cad1 (policy_cad1) (Relational)`.

Some discovery scenarios or templates are provided by default, including the following:

### GDPR [template]

The GDPR [template] scenario provides the latest set of discovery rules and language support for your GDPR compliance strategy. Templates can be copied or edited and saved under a different name, and the GDPR [template] will always receive the latest GDPR discovery rules and language support.

### GDPR

The GDPR scenario provides a basic set of discovery rules that can be used as part of a GDPR readiness strategy. You can edit and save changes to the GDPR scenario, but the scenario will not receive updated rules or language support over time.

Important: If the GDPR [template] is available, using the older GDPR scenario is not recommended because the GDPR scenario does not receive updates.

When editing a pre-defined discovery template and saving the changes, Guardium automatically saves the scenario under a unique name in the format `Copy [timestamp] of [discovery template name]`. For example, editing and saving the GDPR [template] scenario results in a discovery scenario named `Copy [2018-01-01 12:00:00] of GDPR [template]`.

Next topic: [Name and description](#)

## Name and description

Provide a name and description for your discovery scenario.

### About this task

During this step, you may also specify *security roles* that can access the discovery scenario.

### Procedure

1. Open the Name and Description section and provide or edit the name and optional description of the scenario.
2. Create or select a classification policy to use with the discovery scenario.
  - Click the  icon to name a new classification policy. The classification policy is created when saving the discovery scenario.
  - Use the drop-down menu to select an existing classification policy. Rules for the classification policy are automatically loaded into the What to discover section of discover sensitive data tool. When selecting and editing a pre-defined classification policy, Guardium automatically saves the policy under a unique name in the format `Copy [timestamp] of [policy template name]`. For example, editing and saving the GDPR [template] policy results in a classification policy named `Copy [2018-01-01 12:00:00] of GDPR [template]`.
3. Provide category and the classification labels for tagging violations.  
"Sensitive" is the default value for category and classification labels.
4. Use the Datasource type menu to identify the type of datasources used with the scenario.  
For example, select Relational (SQL) for relational databases like MySQL or Document for document-type databases like MongoDB. It is not possible to use multiple datasource types in the same discovery scenario.
5. Optionally, click the Roles button to specify *security roles* that can access the discovery scenario.

### What to do next

Continue to the next section of the discovery scenario, What to discover.

**Previous topic:** [Discovery scenarios](#)

**Next topic:** [What to discover](#)

## What to discover

Create policies consisting of rules and rule actions for discovering and classifying sensitive data.

### About this task

*Classification policies* contain ordered sets of rules and rule actions that identify and take actions on sensitive data. Each rule in a policy defines a conditional action that is taken when the rule matches. The conditional test can be simple, for example a wildcard string found anywhere in a table or collection, or a complex test that considers multiple conditions. For discover sensitive data scenarios, the action triggered by a rule can be a grouping action that adds the matches to a specified group or an alerting action that triggers a notification. Multiple grouping and alerting actions can be combined and ordered to create sophisticated responses to matched rules.

This task guides you through the processes of creating and editing classification rules and rule actions for use in your discovery scenario.

### Procedure

1. Open the What to discover section to define rules for discovering data.
2. Use the Language menu to filter rule templates by the selected language and countries where the selected language is a national language.  
Templates for universal patterns like credit card numbers and email addresses are displayed for all Languge menu selections.
3. Add rules to your discovery scenario or edit existing rules by doing one of the following:
  - Click the  icon to create a new rule.
  - Select rules from the Classification Rule Templates table and click the  icon to add predefined rules.
  - Click the  icon to edit an existing rule.
4. When adding or editing classification rules, use the following procedure.
  - a. Select a Rule type based on the type of search being performed.
    - Search for data matches specific patterns or values in the data.The following data types are supported when searching for data:

|             |           |
|-------------|-----------|
| BIGINT      | NUMERIC   |
| CHAR        | NVARCHAR  |
| DATE        | NVARCHAR2 |
| DECIMAL     | REF       |
| DOUBLE      | SMALLINT  |
| FLOAT       | TIME      |
| INTEGER     | TIMESTAMP |
| LONGVARCHAR | TINYINT   |
| NCHAR       | VARCHAR   |
| NUMBER      | VARCHAR2  |
  - For relational-type datasources, Catalog search matches table or column names in the database. For document-type datasources, Catalog search matches collection or field names in the database.

- Search for unstructured data matches specific values or patterns in an unstructured data file, for example CSV, TXT, or CEF files. Search for unstructured data rules only work with datasources using the database type TEXT.
- b. Provide a name and description while optionally specifying a *special pattern test* at the beginning of the Name field. The rule name will also be used to name the rule associated with the classification policy in the Classification Policy Builder. If you require a special pattern test, it is recommended that you work with its corresponding template (for example, use Bank Card - Credit Card Number for credit card numbers).
- c. Open the Rule Criteria section to define a *regular expression* and other search criteria for the rule. If you are working with a rule template, an appropriate *regular expression* is provided by default.
- Attention: For rules created in the discover sensitive data scenario, the default Data type includes both Number and Text.
- d. Open the Actions section and define any *rule actions* that should be taken when rule criteria match.
- e. When defining multiple *rule actions*, you can optionally click the  icon and use the  and  icons to change the order in which the actions are executed.
- Note: The Ignore and Log result *rule actions* cannot be combined with other *rule actions* and must be used as the only action in a rule. The Log policy violation *rule action* can only be used once in a rule.
- f. Click Save when you are finished adding or editing rule definitions to return to the What to discover section of the discovery scenario.
5. Optionally click the  icon and use the  and  icons to change the order in which rules are applied. Rule order is important as the default behavior stops rule execution after the first match unless Continue on match is selected under Rule criteria.

## What to do next

Continue to the next section of the discovery scenario, Where to search.

**Previous topic:** [Name and description](#)

**Next topic:** [Where to search](#)

## Related concepts

- [Regular Expressions](#)

## Related reference

- [Actual Member Content](#)
- [Rule Criteria](#)
- [Special pattern tests](#)

## Rule Criteria

This topic describes classification rule criteria.

The rule criteria displayed in the Discover Sensitive Data interface reflect the datasource-type defined for the scenario. Not all classification rule criteria are available for all datasource types. For example, the Relational (SQL) datasource type includes rule criteria for Compare to values in SQL while the Document datasource type does not.

Table 1.

| Attribute                  | Description                                                                                                                                                                                                                                                  |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Table type                 | Select one or more table types to search: Synonym, Table, or View. Table is selected by default.                                                                                                                                                             |
| Collection type            | Select one or more collection types to search: Collection or View. Collection is selected by default.                                                                                                                                                        |
| Data type                  | Select one or more data types to search: Number, Text, or Date. Number and Text are selected by default.                                                                                                                                                     |
| Search expression          | Optionally enter a regular expression to define a search pattern to match. To test a regular expression, click the RE button to open the regular expression editor.                                                                                          |
| Table name like            | Optionally enter a specific name or wildcard pattern. If omitted, all table names are selected.                                                                                                                                                              |
| Collection name like       | Optionally enter a specific name or wildcard pattern. If omitted, all collection names are selected.                                                                                                                                                         |
| Column name like           | Optionally enter a specific name or wildcard pattern. If omitted, all column names are selected.                                                                                                                                                             |
| Field name like            | Optionally enter a specific name or wildcard pattern. If omitted, all field names are selected.                                                                                                                                                              |
| Continue on match          | If the next rule in the classification policy should be evaluated after this rule is matched, mark the Continue on Match checkbox. The default is to stop evaluating rules once a rule is matched.                                                           |
| One match per column       | When continuing after a match, evaluate subsequent rules only on columns not matched by a previous rule.                                                                                                                                                     |
| One match per field        | When continuing after a match, evaluate subsequent rules only on fields not matched by a previous rule.                                                                                                                                                      |
| Calculate confidence score | Calculate confidence score during scanning. It is calculated as hits/sample size. Calculating a confidence score impacts the performance of the scan.                                                                                                        |
| Search wildcard            | Optionally enter a specific value or a wildcard pattern. If omitted, all values are selected.                                                                                                                                                                |
| Minimum length             | Optionally enter a minimum length. If omitted, there is no limit.                                                                                                                                                                                            |
| Maximum length             | Optionally enter a maximum length. If omitted, there is no limit.                                                                                                                                                                                            |
| Evaluation name            | Optionally enter a fully qualified Java™ class name that has been created and uploaded. The Java class will then be used to fire and evaluate the string. Note: There is no validation that the class name entered was loaded and conforms to the interface. |

| Attribute                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fire only with marker      | <p>The Fire only with marker allows for the grouping of classifier rules: rules with the same marker fire at the same time. Additionally, all returned rules using a marker must return data based on the same table or collection name. If two or more rules are defined with the same marker, those rules will fire together such that if both rules fire on the same table or collection they will both be logged and their actions invoked. On the other hand, if only one rule fires on a table or collection then neither of the rules will be logged or have their actions invoked. Being able to have multiple rules fire together becomes important when you care about sensitive data appearing together within the same table or collection. For example, you may want to know when a table or collection has both a social security number and a Massachusetts drivers license.</p> <p>The fire only withMarker is a constant value, can be named to any value, and must have the exact same value across the rules you want grouped. This means that if one rule has a marker of ABC then the other rule that you want to group it with must also have a marker named ABC.</p> <p>The Fire only with Marker also interacts with the Continue on Match flag. For example, if the following rules were defined such that Rule 3 does not match the Continue on match then no results will be returned regardless if all three marker rules were positive. This is because you didn't get to run Rule 4 and the grouping will not fire because all Fire only with markers must execute with positive results.</p> <p>Rule 1. Firemarker rule "ABC" (continue on match)</p> <p>Rule 2. Firemarker rule "ABC" (continue on match)</p> <p>Rule 3. Firemarker rule "ABC" (continue on match)</p> <p>Rule 4. Firemarker rule "ABC" (continue on match)</p> |
| Hit percentage             | Optionally enter a percentage of matching data that should be achieved for this rule to fire. Data is returned if the percentage of matching data examined is greater than or equal (>=) then the percentage value entered, noting that an empty entry means it is not a condition and will not affect whether the rule fires or not and return data to the view screen. A 0 percentage will cause the rule to fire for this condition and return data to the view screen, and a percentage of 100 requires that all must match.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Compare to values in SQL   | <p>Optionally enter a SQL statement. The SQL entered, which must be based on returning information from one and only one column, will then be used as a group of values to search against the tables and columns selected.</p> <p>Note: If used, the Compare to values in SQL should observe the following rules:</p> <ul style="list-style-type: none"> <li>The SQL statement MUST begin with <b>SELECT</b>.</li> <li>The SQL statement SHOULD NOT utilize the ; (semi-colon).</li> <li>The SQL entered MUST specify a schema value name in order to be accurate in returning results.</li> <li>Good examples:</li> </ul> <pre>SELECT ename FROM scott.emp select EMPNUMBER from SYSTEM.EMP where EMPNUMBER in(5555,4444) select DNAME from SCOTT.DEPT where DNAME like 'A%G' SELECT ZIP from SCOTT.FOO where ZIP in (SELECT ZIP FROM SCOTT.FOO)</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Compare to values in group | Optionally select a group. The group selected will then be used as a group of values to search against the tables and columns selected. As long as one of the values within a group, that is either a public or a classifier group, matches, then the value rule will return data.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Show unique values         | Mark the Show Unique Values checkbox to add details on what values matched the classification policy rules to the comments field of the resulting report. The row count for each match is indicated in parenthesis following the value. For example, 3 <b>matched distinct values [1662 (1), 436 (3), 629 (27)]</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Unique values mask         | Use regular expressions in the Unique values mask field to redact the unique values. For example, mark the Show unique values checkbox and use <b>([0-9] {2} - [0-9] {3}) - [0-9] {4}</b> in the Unique values mask field to log the last four digits and redact the prefix digits.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Exclude schema             | Optionally select a group of schema to exclude.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Exclude table              | Optionally select a group of tables to exclude.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Exclude table column       | Optionally select a group of table columns to exclude. The following wildcard character is supported: %                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Actual Member Content

Use the Actual Member Content field to define how objects are labeled by the Add to Group of Objects rule action.

Table 1.

| Actual Member Content Selection | Value in Group              |
|---------------------------------|-----------------------------|
| Object Name Only                | tableName                   |
| Like Name%                      | tableName%                  |
| Like %Name                      | %tableName                  |
| Like %Name%                     | %tableName%                 |
| %/%.Name                        | %/.tableName                |
| Fully Qualified Name            | schemaName.tableName        |
| Like Full%                      | schemaName.tableName%       |
| Like %Full                      | %schemaName.tableName       |
| Like %full%                     | %schemaName.tableName%      |
| %/Full                          | %/.schemaName.tableName     |
| Read/%.Name                     | Read/%.tableName            |
| Change/%.Name                   | Change/%.tableName          |
| Read/Full                       | Read/schemaName.tableName   |
| Change/Full                     | Change/schemaName.tableName |

If your rules return the table name **JJ\_CREDIT\_CARD** from the schema **DB2INST1**, and you have specified an Add to Group of Objects action, the Actual Member Content selections behaves as follows:

- Selecting Fully Qualified Name adds `DB2INST1.JJ_CREDIT_CARD` to the selected group.
- Selecting Object Name Only adds `JJ_CREDIT_CARD` to the selected group.
- Selecting Change/Full adds `Change/DB2INST1.JJ_CREDIT_CARD` to the selected group.

## Where to search

Identify datasources to scan for sensitive data.

## About this task

Datasources store information about your database or repository such as the type of database, the location of the repository, or authentication credentials that may be associated with it. Adding datasources to a discovery scenario creates a *classification process* where *classification policies* are applied to the selected datasources.

In this task, identify the datasources you would like to search for sensitive data.

## Procedure

1. Open the Where to search section to identify the datasources you would like to search for sensitive data.
2. Add datasources to your discovery scenario by doing one of the following:
  - Click the  icon to open the Create Datasource dialog and add a new datasource definition.
  - Select datasources from the Available Datasources table and click the  icon to add existing datasources. Note that the list of datasource is filtered by the datasource type defined for the scenario. For example, scenarios using the `Relational (SQL)` datasource type only list relational-type datasources.
  - Select a group from the Available datasource groups table and click the  icon to add a group of datasources. For groups containing multiple types of datasources, only datasources matching the datasource type defined for the scenario are used. For example, scenarios using the `Document` type datasource only use `Document` type datasources and ignore any `Relational` type datasources that exist in the group.
3. Define a new datasource, or edit an existing datasource by selecting the datasource and clicking the  icon.  
New datasources defined through the discovery scenario can also be viewed or edited through the Datasource Definitions tool.
  - a. Provide or edit the name of the datasource.
  - b. Select the appropriate database type from the Database type menu and provide the requested information to complete the datasource definition.  
The available fields differ depending on the selected database type. Note that the list of database types is filtered by the datasource type defined for the scenario. For example, scenarios using the `Relational (SQL)` datasource type only list relational-type databases.
  - c. When you are finished editing the datasource definition, click Save to save your work and optionally click Test Connection to verify the datasource connection.
  - d. When you are finished working with the datasource definition, click Close to close the dialog.
4. If you are using this classification process for cloud databases also, select Enable object auditing for Cloud DBs.

## Results

A *classification process* is created after adding datasources to your discovery scenario and saving the scenario. To view or edit this process directly, use the Classification Process Builder.

## What to do next

Continue to the next section of the discovery workflow, Run discovery.

**Previous topic:** [What to discover](#)

**Next topic:** [Run discovery and review report](#)

## Related concepts

- [Datasources](#)

## Related tasks

- [Creating a datasource definition](#)
- [Configuring custom properties for your datasources](#)

## Run discovery and review report

Optionally run your discovery scenario and review the results.

## About this task

After defining policies for discovering sensitive data and identifying datasources to search, you can run the *classification process* and review the results. Running the process and reviewing the results allows you to refine your policies, for example specifying additional search criteria if you find the results too broad. It may be necessary to go through several iterations of refining policies, running the process, and assessing the results before achieving the desired results.

## Procedure

1. Open the Run discovery section to test your discovery scenario.
2. Click Run Now to begin.

Attention:

- Depending on the policies you have specified and the number of datasources you have selected to search, it may take several minutes or more to complete the process of identifying sensitive data. The process status is indicated next to the Run Now button, or you can monitor the process using the Guardium Job Queue.

If progress indication does not begin and the Run Now button becomes enabled without indicating that results are available, save the scenario and try running the job again.

- By default, the classifier uses `count *` to determine cardinality for random sampling. For Oracle datasources, Guardium also supports using database statistics to determine cardinality. For more information, see the DATA-CARDINALITY-FOR-SAMPLING-TABLES = STATISTICS custom property in the [Oracle \(Data Direct - SID\)](#) or [Oracle \(Data Direct - Service Name\)](#) documentation.

3. When the discovery scenario has finished running, open the Review report section to see the results.

- Use the Generation time menu to select the report instance to view.

- The  icon lists the datasources included in the report.
- Click the  icon to adjust report settings such as aliases and hierarchical groups.
- Open the Process log to review detailed log information.
- Use the Filter box to refine results (filtering is not supported with more than 10,000 results).

4. While reviewing the results, you can define additional rules and actions based on the results.

- a. Select the row(s) containing data you want to define actions against.
- b. Click Add to Group to define a grouping action, or click Advanced Actions to define other actions such as alerting, logging, or ignoring.
- c. After completing the dialog to define an action, click OK to return to the results report.

Attention:

- Actions added from the results table are considered ad hoc actions that run only as invoked from the results table. These actions will not appear in the [What to discover](#), [Edit rule](#), [Actions](#) section of your discovery scenario, and they will not run automatically as part of the discovery scenario or related *classification processes*.
- Use the Policy Builder to review, edit, and install alerting actions and access rules.
- Use the Group Builder to review and edit grouping actions.
- Use the Privacy Set Builder for to review privacy set actions.
- Use the Incident Management tool to review policy logging actions.

## Results

---

After running the search for sensitive data, monitor its status next to the Run Now button or using the Guardium Job Queue. You can use the Group Builder to review any grouping actions or the Policy Builder to review and install any alerting actions that were added from the results table.

## What to do next

---

Optionally, continue to the next section of the discovery scenario, Audit.

- [Remove false-positives from discovery results](#)

Learn how to mark false-positives in your discovery results and prevent them from appearing in future scans.

Previous topic: [Where to search](#)

Next topic: [Audit](#)

---

## Remove false-positives from discovery results

Learn how to mark false-positives in your discovery results and prevent them from appearing in future scans.

### About this task

---

After defining policies for discovering sensitive data and identifying datasources to scan, you can run the discovery scan and review the results. While reviewing results of a discovery scan, you may find some false-positive matches in the results. You can add these false positives to an exclusion group so they are ignored in subsequent scans. If automatically populating a sensitive objects group based on discovery scan results, removing false positives from that sensitive objects group ensures that actions or policies defined for that group function correctly.

This example uses a discovery scenario with relational-type datasources, but the procedure applies to all datasource types with minor differences. For example, relational-type scenarios use the Add to group of tables to exclude action while document-type scenarios use the Add to group of collections to exclude action.

### Procedure

---

1. Navigate to Discover > Classification > Discover Sensitive Data and select the discovery scenario to review.
2. Review discovery scan results and add false-positives to exclusion groups.
  - a. Click to open the Review report section and see the results of the discovery scan.  
If there are no results, this may mean that the discovery process has not yet run. Click to open the Run discovery section to see the last-run timestamp.
  - b. In the results table, select one or more rows containing false-positive data and click the Add to group button to define a grouping action.  
Group for exclusion based on the granularity of the selected data:
    - Add to Group of Schemas to Exclude
    - Add to Group of Tables to Exclude
    - Add to Group of Tables/Columns to Exclude  
It is possible to add one false-positive to an exclusion group of schemas and another false-positive to an exclusion group of tables or columns.
  - c. Use the Select Exclude Group dialog to select or create an exclusion group.
  - d. Click OK to close the dialog and return to the discovery results table.

#### Attention:

- The original results remain in the table after adding false-positive data to exclusion groups. This is because the result viewer shows the results of the most recent discovery scan. To ensure that the objects have been added, review the exclusion group members using the Group Builder.
- Actions performed from the results table are considered ad hoc actions that run only as invoked from the table. These actions will not appear in the What to discover > Edit rule > Actions section of the discovery scenario, and they will not run automatically as part of the discovery scenario or related classification processes.

### 3. Add exclusion groups to the rule that triggered the false-positive match.

- a. In the Review report section, use the Rule description column in the results table to identify which rule matched the false-positive data.
- b. Click to open the What to discover section and select the rule from the Selected classification rules table. Click the icon to begin editing the rule.
- c. From the Edit rule page, click to open the Rule criteria section, and click the Show advanced options link.
- d. Add the exclusion group to either the Exclude schema, Exclude table, or Exclude table column parameter. Choose the granularity that matches your selection for the false-positives in the discovery results.
- e. Click the Save button to save the rule.
- f. Click the Save button to save the discovery scenario.

### 4. Remove false-positive data from the sensitive objects group.

Discovery template rules automatically add matches to a sensitive objects group, and your own rules may define a similar behavior. To prevent the false-positives from appearing in future discovery scans, remove the false-positive data from the sensitive object group.

- a. Navigate to Setup > Tools and Views > Group Builder.
- b. Select the appropriate sensitive objects group and click the icon.
- c. On the Members tab of the Edit group dialog, select the false-positives and click the icon.
- d. Click the Save button to update the group.

## Results

The next time you run the discovery scenario, the false-positives identified using this procedure will not appear as matches.

## Audit

Optionally create an audit process by defining receivers, a distribution sequence, and review options for the discovery and classification report.

## About this task

You can define any number of receivers for the results of a discovery workflow, and you can control the order in which they receive results. In addition, you can specify process control options, such as whether a receiver needs to sign off on the results before they are sent to the next receiver.

## Procedure

1. Open the Audit section to define receivers for discovery reports.
2. Use the Audit process menu to select an audit process to use with the discovery scenario.  
When creating a new discovery scenario, a new audit process name is suggested in the format of [scenario name] Audit process [timestamp]. For example, creating a scenario named discover\_cadl results in an audit process named disover\_cadl Audit process [2018-01-01 12:00:00].
3. Add receivers to your discovery scenario by clicking the icon and defining options for how the reports are delivered.
  - If sending the report to Guardium users, roles, or groups, you will need to define process control options.
  - If sending the report to email recipients, provide their email address and filter the report by a Guardium username that is appropriate for the email recipient.
4. Click OK to add the receiver to the discovery workflow.  
Continue adding additional receivers to the scenario if needed.
5. Optionally click the icon and use the and icons to change the order in which reports are distributed to recipients. This is important when using sequential distribution as it determines which receivers must review or sign the report before it is sent to subsequent receivers.

## Results

An *audit process* is created after defining receivers and saving the discovery scenario. To view, edit, or run this process directly, use the Audit Process Builder.

The *audit process* remains inactive until it is scheduled using the Schedule section of the discovery scenario or using the Audit Process Builder. You can also run the *audit process* by visiting the Audit Process Builder, selecting the *audit process*, and clicking Run Once Now.

## What to do next

Optionally, continue to the next section of the discovery workflow, Schedule.

**Previous topic:** [Run discovery and review report](#)

**Next topic:** [Scheduling](#)

## Related concepts

- [Building audit processes](#)

## Scheduling

Optionally activate the audit process by scheduling it to run at defined intervals.

## About this task

A schedule becomes part of an *audit process* along with any receivers specified in the Audit section of the discovery scenario. Defining a schedule runs the *audit process* at specified intervals and ensures that results from the associated *classification process* are regularly distributed and reviewed.

## Procedure

1. Open the Schedule section to define a schedule for discovering data.
2. Use the Schedule by menu to set daily or monthly intervals for the *audit process*.
3. Use the Start schedule every and Repeat every check boxes to define how many times per day and how many times within each hour to run the *audit process*.
4. Use the Start date and time controls to define an explicit date and time for the schedule to begin.
5. Clear the Activate schedule check box to deactivate the *audit process* while retaining scheduling information for later use. The Activate schedule box is checked by default, meaning that the audit process becomes active after saving the schedule.
6. When you have defined a schedule, click Save to finish editing and close the workflow editor.

## Results

An *audit process* is created after defining a schedule and saving the discovery scenario. To view or edit this audit process directly, use the Audit Process Builder. Review the Scheduled Jobs report to see the status, start time, and next fire time for scheduled audit tasks.

Previous topic: [Audit](#)

## Related concepts

- [Building audit processes](#)

## Runtime sensitive-object identification

Runtime sensitive-object identification processes response data looking for predefined patterns that match personally-identifiable and other sensitive information.

## About this task

Runtime sensitive-object identification matches user-selectable patterns for data such as credit card numbers, international bank numbers, email addresses, and personal identification numbers for various countries. Use the **Runtime Sensitive Object Identifier** session-level policy to enable runtime sensitive object identification, select patterns to match, and view the results.

Note: If runtime sensitive-object identification is active when you upgrade to Guardium 12.0, the installed rules from your previous version are changed to a migrated **Runtime Sensitive Object Identifier** policy. Use the methods described in [Creating session-level and advanced session-level policies](#) to add or remove patterns, change predefined rules, or copy and create new rules. Pattern names from earlier releases migrate as rule names to Guardium 12.0.

The *IPV6 address and Belgium: National Number* patterns are deprecated and will not migrate to Guardium 12.0.

## Procedure

1. From the Guardium® UI, browse to Security>Security Policies>Policy Builder for Data to open the Security Policies page.
2. From the Security Policies page, select the **Runtime Sensitive Object Identifier [template]**.  
You can either run the policy as is, or make a copy () and customize the policy for your specific needs. For more information about using session-level policies, see [Creating session-level and advanced session-level policies](#).
3. View results using the Runtime Sensitive Object Identifier report.  
You can modify the report to display the information that you need. For more information, see the [Runtime Sensitive Object Identifier](#) report.

## What to do next

You can copy, and then modify the Runtime Sensitive Object Identifier policy as required for your needs. For information about making changes to a policy, see [Creating session-level and advanced session-level policies](#).

## Related information

- [Runtime Sensitive Object Identifier](#)

## Regular Expressions

Regular expressions can be used to search traffic for complex patterns in the data.

The IBM® Guardium® implementation of regular expressions conforms with PCRE. This information does not provide a comprehensive description of how regular expressions are constructed or used. The important point to keep in mind about pattern matching or XML matching using regular expressions is that the search for a match starts at the beginning of a string and stops when the first sequence matching the expression is found. Different or the same regular expressions can be used for pattern matching and XML matching at the same time. For more detailed information, see the PCRE web site: <https://www.pcre.org/>

# FAM discovery and classification in Windows and UNIX-Linux file servers

File activity discovery and classification ensures integrity and protection of sensitive data on UNIX-Linux and Windows file servers.

Restriction: FAM discovery agent (crawler) is only applicable to Guardium® Data Protection versions 11.4, 11.5 and 12.0.

- [Installing and activating the FAM discovery agent \(crawler\) on UNIX servers](#)

Install the GIM client on a UNIX file server, then use it to install the file activity monitoring discovery agent (crawler).

- [Installing and activating FAM discovery agent \(crawler\) on Windows servers](#)

Install the GIM client on the file server, then use it to install the FAM discovery agent.

- [File discovery and classification GIM parameters](#)

These GIM parameters configure file discovery and classification for each collector.

- [Rules for GDPR File Activity](#)

Use the rules listed here to create decision plans for FAM GDPR.

## Installing and activating the FAM discovery agent (crawler) on UNIX servers

Install the GIM client on a UNIX file server, then use it to install the file activity monitoring discovery agent (crawler).

### Before you begin

- Restriction: FAM discovery agent (crawler) is only applicable to Guardium® Data Protection versions 11.4, 11.5 and 12.0.
- License keys must be installed. See [Install license keys](#).
- S-TAP for FAM must be installed. Required for file monitoring and policy enforcement. See [Linux-UNIX: Installing, upgrading and uninstalling S-TAP agents](#).
- Verify that a bash shell is installed.
- Verify that the Compatibility standard C++ libraries i686 package libraries are installed. When running ICC with the incorrect libstdc version, the client will receive a bnsRun error. If the FAM discovery agent is already installed, uninstall and re-install the agent after you install the libraries.
- FAM discovery agent (also known as the FAM bundle or FAM agent) must be accessible. Required for file discovery and classification. Download from [Fix Central](#) or obtain from your Guardium representative.
- Disk space requirements for FAM bundle: 2GB. AIX platforms require an additional 2GB during installation.
- The FAM discovery agent (crawler) does not support TLS encryption.

Tip: To install the FAM discovery agent successfully on AIX, it is recommended to set the process data size to unlimited. Access the file /etc/security/limits and change this line to **default: data = -1**.

### Procedure

1. Install the GIM client on the file server. See [Guardium installation manager](#).
2. Download the FAM bundle and save it in an accessible drive.  
The UNIX bundle has a name like: guard-bundle-FAM\_r\*\*\*\*\*\_trunk\_\*\*\*\*.gim.
3. On the central manager (if there is one), upload and import the FAM bundle. If there is no central manager, upload and import the FAM bundle to the appliance.
  - a. Navigate to [Manage > Module Installation > Upload Modules](#).
  - b. Under [Upload Module](#), click [Browse](#) and navigate to the FAM bundle. Click [Upload](#).
  - c. Under [Import uploaded modules](#), select the FAM bundle and click [Install/Update](#).
4. Install and configure the FAM bundle using [Manage > Module Installation > Set up by Client](#).  
For more information on GIM, see [Set up by Client](#).
  - a. To enable the FAM monitor, set [STAP\\_FAM\\_ENABLED](#) to 1 (enabled). This is required even if you are only using the FAM discovery agent.
  - b. FAM discovery is enabled by default ([FAM\\_ENABLED](#)).  
Configure additional parameters as relevant.
    - Configure [SOURCE\\_DIRECTORIES](#) for the directories you want to scan.
    - By default, the agent performs basic scanning for entitlement information. To enable scanning based on decision plans, such as for SOX or HIPAA, set [FAM\\_IS\\_DEEP\\_ANALYSIS](#) to true. By default, it uses all of the default decision plans. You can specify which decision plans you want it to use.
    - The default schedule for the scanning is every 12 hours, and starts immediately upon configuration. You can change these using GIM parameters [FAM\\_SCHEDULER\\_HOUR\\_INTERVAL](#), [FAM\\_SCHEDULER\\_START](#), [FAM\\_SCHEDULER\\_REPEAT](#).See full parameter list in [File discovery and classification GIM parameters](#).
5. Verify that the FAM discovery agent installed successfully by viewing the Guardium S-TAP Status Monitor report (add the report from My Dashboards). Look for the [FAM\\_Agent](#) suffix in the IP address of the S-TAP host.
6. To trigger file rediscovery later without uninstalling and reinstalling the FAM bundle:
  - a. Remove the files under the work directory. If Guardium is installed in the default directory, the files to be removed are in this directory on the file server: [/usr/local/IBM/modules/FAM/current/files/work](#)
  - b. Change any FAM parameters in GIM, for example, changing the time interval from 5 to 10 minutes.
  - c. Click [Apply to Selected](#) then click [Install/Update](#).

### Results

Discovery and Classification results: After you install the FAM discovery agent (file crawler), a basic run of the file crawler begins, using the initial path that you specified during the installation. Each time the crawler completes its run, it sends a status message that is included in the Files Crawler Configuration report. This process gathers the list of folders and files, their owner, access permissions, size, and the time and date of the last update.

### Related reference

- [File Activity Monitor APIs](#)

# Installing and activating FAM discovery agent (crawler) on Windows servers

Install the GIM client on the file server, then use it to install the FAM discovery agent.

## Before you begin

- Restriction: FAM discovery agent (crawler) is only applicable to Guardium® Data Protection versions 11.4, 11.5 and 12.0.
- License keys must be installed. See [Install license keys](#).
- FAM discovery agent (also known as the FAM crawler or FAM agent) must be accessible. Required for file discovery and classification. Download from [Fix Central](#) or obtain from your Guardium representative.
- Either a Windows S-TAP or the Windows FAM Monitor must be available.
- Verify that the Compatibility standard C++ libraries i686 package libraries are installed.
- .NET 4.5 or above is installed. If not yet installed, .NET 4.5 requires 5 GB.
- Disk space requirements: 2GB.
- The FAM discovery agent (crawler) does not support TLS encryption.

The FAM monitor package is a standalone package, and is installed independently. When upgrading from 11.0 and higher:

- If you're using FAM and S-TAP:
  1. Upgrade the S-TAP to your current version. This uninstalls the previous FAM (FsMonitor driver and StapAT service).
  2. Install the FAM crawler and FamMonitor.
- If you're using FAM only:
  1. Uninstall the S-TAP. This uninstalls the previous FAM (FsMonitor driver and StapAT service).
  2. Install the FAM crawler and FamMonitor.

## Procedure

1. Make sure that the following Guardium features are installed:
    - The GIM client on the file server. For more information, see [Installing the GIM client on a Windows server](#)
    - An S-TAP, the FAM Monitor, or both. For more information about installing the FAM Monitor, see [Installing and activating the FamMonitor on Windows servers](#)
  2. Download the FAM bundle and save in an accessible drive.  
The monitoring and discovery agent bundle name has the format: guard-FAM-guardium\_r\*\*\*\*\*Windows-Server-x86\_x64\_ia64.gim.
  3. On the central manager if there is one, otherwise on an appliance, upload and import the FAM discovery agent bundle.
    - a. Browse to Manage > Module Installation > Upload Modules.
    - b. Under Upload Module, click Browse and navigate to the FAM bundles. Click Upload.
    - c. Under Import uploaded modules, select the FAM bundles and click Install/Update.
- Configure additional parameters as relevant:
- Note: You can also configure GIM parameters using the grdapi command: **gim\_update\_client\_params**.
- Configure SOURCE\_DIRECTORIES for the directories you want to scan.
  - By default, the agent performs basic scanning for entitlement information. To enable scanning based on decision plans, such as for SOX or HIPAA, set FAM\_IS\_DEEP\_ANALYSIS to true. By default, it uses all of the default decision plans. You can specify which decision plans you want it to use.
  - The default schedule for the scanning is every 12 hours, and starts immediately upon configuration. You can change these using GIM parameters FAM\_SCHEDULER\_HOUR\_TIME\_INTERVAL, FAM\_SCHEDULER\_START, FAM\_SCHEDULER\_REPEAT.
- See full parameter list in [File discovery and classification GIM parameters](#).
4. Verify that the FAM discovery agent installed successfully by viewing the Guardium S-TAP Status Monitor report (add the report from My Dashboards). Look for the FAM\_Agent suffix in the IP address of the S-TAP host.
  5. To trigger file rediscovery later without uninstalling and reinstalling the FAM bundle:
    - a. Remove the files under the work directory. If Guardium is installed in the default directory, the files to be removed are in this directory on the file server: /usr/local/IBM/modules/FAM/current/files/work
    - b. Change any FAM parameter in GIM, for example, changing the time interval from 5 to 10 minutes.
    - c. Click Apply to Selected then click Install/Update.

## Results

When the installation of the FAM discovery agent (file crawler) is complete, a basic run of the file crawler begins, using the initial path that you specified during the installation. Each time the crawler completes its run, it sends a status message that is included in the Files Crawler Configuration report. This process gathers the list of folders and files, their owner, access permissions, size, and the time and date of the last update.

## Related concepts

- [Investigation Dashboard for files](#)

## Related tasks

- [GIM Set up by Client](#)
- [Enabling File Activity in the investigation dashboard](#)
- [Installing and activating the FamMonitor on Windows servers](#)

## Related reference

- [GuardAPI File Activity Monitor Functions](#)

## File discovery and classification GIM parameters

These GIM parameters configure file discovery and classification for each collector.

Configure file discovery and classification per collector. These parameters can be configured during installation, or later using GIM (Manage > Module Installation > Set up by Client) or using the GuardAPI command **gim\_update\_client\_params**. You can only update one collector at a time when using the GuardAPI.

| GIM Parameter                       | client.ini                     | Default | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | GUI |
|-------------------------------------|--------------------------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| FAM_CLASSIFICATION_LANGUAGE         |                                | English | <p>Set to GenericLanguage for automatic language detection.</p> <p>For Linux, ensure that your Linux server has the required language support that is installed. For example, to support Chinese document classification, Chinese support should be installed on Linux.</p> <p>For more information about supported languages for IBM Content Classification, see <a href="https://www.ibm.com/support/knowledgecenter/SSBRAM_8.8.0/com.ibm.classify.workbench.doc/c_WBG_available_languages.htm">https://www.ibm.com/support/knowledgecenter/SSBRAM_8.8.0/com.ibm.classify.workbench.doc/c_WBG_available_languages.htm</a></p>                                                                                                                             | X   |
| FAM_DEBUG                           | logger.debugLevel              | 0       | <p>Logs on the file server are collected and sent to the Guardium appliance.</p> <p>0=OFF<br/>1=ON</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | X   |
| FAM_ENABLED                         |                                | 1       | <p>Enables FAM discovery. UNIX only.<br/>0 = FAM Discovery agent is disabled.<br/>1 = FAM Discovery agent is enabled. This is the default.<br/>2 = Restart FAM Discovery agent.</p> <p>To restart FAM: Change the FAM_ENABLED parameter in the GIM GUI to 2 and apply to clients by clicking Install/Update.</p> <p>The FAM service in the file server should change PID showing it has restarted (<b>ps -ef   grep fam</b>), and there is a new entry in the pre-defined GUI report "Files Crawler Configuration".</p> <p>The config reverts to 1 in the GIM GUI allowing you to restart again by repeating the process.</p> <p>The S-TAP parameter <b>fam_enable</b> must be enabled for the discovery agent to function.</p>                             | X   |
| FAM_ICM_CLASS_DECISION_PLANS        |                                |         | <p>Enable the decision plans by including their plan names and classification entities.</p> <p>Format:</p> <ul style="list-style-type: none"> <li>• List the entities for each decision plan, delimited by colons.</li> <li>• For each decision plan, list the entities in curly braces and comma-delimited</li> </ul> <pre>DecisionPlanName1(Entity1.1,Entity1.2,...):DecisionPlanName2(Entity2.1,Entity2.2,...)</pre> <p>If the curly braces are empty or missing for some Decision Plans, all classification entities are presented in the classification results in FAM report /Investigation Dashboard. Examples with empty or missing curly braces:</p> <pre>DecisionPlanName1():DecisionPlanName2()<br/>DecisionPlanName1:DecisionPlanName2"~"</pre> | X   |
| FAM_ICM_CLASS_THREAD_COUNT          |                                | 5       | Number of threads for the classifier to use. The default is 5 and is the recommended value.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | X   |
| FAM_ICM_URL                         | http://localhost:18087         |         | The URL of the IBM Content Classification Server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | X   |
| FAM_INSTALLED                       |                                | 0       | If you want to enable FAM, set the S-TAP parameter <b>fam_installed</b> to 1 while installing and upgrading STAP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |     |
| FAM_INSTALLER                       |                                |         | The path to the installer package. Windows only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |     |
| FAM_INSTALL_DIR                     |                                |         | The location in which the File Activity Monitoring software is installed. Windows only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |     |
| FAM_IS_DEEP_ANALYSIS                | classifier.isDeepAnalysis      |         | <p>Controls classification</p> <p>False=classification is disabled. Basic scan of metadata and access permission only.</p> <p>True=classification is enabled, based on file content.</p> <p>If no decision plans are enabled (FAM_ICM_CLASS_DECISION_PLANS is undefined), only a basic scan is performed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                               | X   |
| FAM_SCAN_EXCLUDE_DIRECTORIES        | scan.exclude.directories       | NULL    | <p>Directories to exclude from discovery and classification.</p> <p>Format: full path to directory<br/>Wildcards are not supported.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | X   |
| FAM_SCAN_EXCLUDE_REMOTE_DIRECTORIES | scan.exclude.remoteDirectories | true    | <p>Remote directories to exclude from discovery and classification.</p> <p>true: do not scan remote directories.<br/>false: scan remote directories.</p> <p>Wildcards are not supported.</p> <p>On Windows, set to something like: \\RemoteMachine\sharefolder\directory</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | X   |
| FAM_SCAN_EXCLUDE_EXTENSIONS         | scan.exclude.extensions        | NULL    | <p>Excludes the specified file extension(s) or documents without extensions from the FAM scan.</p> <p>Relevant for both Windows and Linux.</p> <p>Format: semicolon delimited list</p> <p>The setting is case sensitive. Examples of excluded extensions: pdf;txt;doc. To exclude documents without extension, set to "NO_EXTENSION".</p>                                                                                                                                                                                                                                                                                                                                                                                                                   | X   |
| FAM_SCAN_EXCLUDE_FILES              | scan.exclude.files             | NULL    | <p>Files to exclude from discovery and classification.</p> <p>Format: valid filename in full path format.</p> <p>Wildcards are not supported.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | X   |

| GIM Parameter                      | client.ini                    | Default | Description                                                                                                                                                                                                                                                                                                                                                         | GUI |
|------------------------------------|-------------------------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| FAM_SCAN_MAX_DEPTH                 | scan.maxDepth                 |         | Limit the depth for the scan relative to the specified starting directories (FAM_SOURCE_DIRECTORIES).                                                                                                                                                                                                                                                               | X   |
| FAM_SCHEDULER_HOUR_TIME_INTERVAL   | scheduler.timeInterval.hour   | 12      | Frequency, in hours, at which the discovery and classification scan is run.<br>Format: integer<br>The default is 12 hours.                                                                                                                                                                                                                                          | X   |
| FAM_SCHEDULER_MINUTE_TIME_INTERVAL | scheduler.timeInterval.minute |         | Along with the hour interval, this is the time interval between scans. For example, if you want scans to occur 12 hours and 30 minutes apart, specify 12 for FAM_SCHEDULER_HOUR_TIME_INTERVAL and 30 for FAM_SCHEDULER_MINUTE_TIME_INTERVAL.<br>Format: integer                                                                                                     | X   |
| FAM_SCHEDULER_REPEAT               | scheduler.repeat              |         | True = Repeat the discovery process at the specified time interval.<br>False = Do not repeat scan.                                                                                                                                                                                                                                                                  | X   |
| FAM_SCHEDULER_START_TIME           | scheduler.startTime           | NULL    | Time of initial activation of the discovery and classification processes.<br>Format: MM-DD-YYYY HH:mm<br>For example, if you enter 01-02-2016 18:00, the scan will start at 6 PM on January 2nd 2016. If the time interval is 12 hours, the process will run every day at 6 PM and 6 AM.                                                                            | X   |
| FAM_SERVER_PORT                    | serverSettings.port           | 16022   | The Guardium collector port, 16022.                                                                                                                                                                                                                                                                                                                                 | X   |
| FAM_SOURCE_DIRECTORIES             | sourceDirectories.paths       | NULL    | The directory or directories to start scanning from.<br>Wild cards are not supported. Example: /home/test.<br>Format: Set list of semicolon delimited FAM source directories.<br>Example: %IBM_FAM_HOME%/test/dir1;%IBM_FAM_HOME%/test/dir2 ~<br>Use FILE_SYSTEM_ROOTS to scan all files in the server. Not recommended especially if the server has lots of files. | X   |

## Related concepts

---

- [GIM - GUI](#)
- [GIM - CLI](#)

## Rules for GDPR File Activity

Use the rules listed here to create decision plans for FAM GDPR.

Address  
Age  
BankAccount  
BelgianID  
Canada\_SIN  
CC\_Amex  
CC\_Diners\_Club  
CC\_Discover\_Club  
CC\_InstaPayment  
CC\_JCB  
CC\_Laser  
CC\_Maestro  
CC\_MasterCard  
CC\_Switch  
CC\_Visa  
Confidential\_match  
CreditCard  
DateOfBirth  
DNI  
EmailAddress  
EmailAll  
EnglishGDPR  
EULA  
Firearm  
FirearmModels  
French\_INSEE  
FrenchAddress  
FrenchBanking  
FrenchCreditCard  
FrenchDOB  
FrenchDriverLicense  
FrenchGDPR  
FrenchID  
FrenchIP  
FrenchLicensePlate  
FrenchMedical  
FrenchPassport  
FrenchPhone  
GDPR\_match  
GenericMedical

GermanAddress  
GermanBanking  
GermanCreditCard  
GermanDOB  
GermanDriverLicense  
GermanEmail  
GermanGDPR  
GermanIP  
GermanLicensePlate  
GermanMedical  
GermanNatID  
GermanPassport  
GermanPhone  
GermanSSN  
GermanTaxID  
GermanVAT  
HumanAttributes  
InternetEmail  
IPAddress  
ITAAircraft  
ITAAircraftModels  
ITARExplodes  
ITARExplodesType  
ItTaxCode  
LegalDocuments  
License  
MedicalDiseases  
MedicalRecords  
Name  
nameMatch  
NI  
NIE  
NIN  
NINO\_UK  
PassportApp\_Can  
PassportApp\_USA  
PESEL  
Phone  
Photo  
PolandID  
PolandNatID  
PrescriptionDrugs  
PrescriptionDrugsPrimary  
PrescriptionDrugsSecondary  
Religion  
Sex  
SexualOrientation  
SocialNetwork  
SpainAddress  
SpainBanking  
SpainCreditCard  
SpainDOB  
SpainDriverLicense  
SpainEmail  
SpainGDPR\_ST  
SpainIP  
SpainLicensePlate  
SpainMedical  
SpainNatID  
SpainPassport  
SpainPhone  
SpainSSN  
SpainTaxID  
SpainVAT  
SSN  
TaxEIN\_SSNSummary  
TaxEIN\_Summary  
TaxSSN\_Summary  
UK\_NHS  
UKLicense  
UKPhoneNum  
URL  
US\_SSNS  
USPhoneNum  
VisaApplication

---

## File discovery and classification for NAS and SharePoint

File Discovery, Entitlement and Classification (FDEC) for NAS and SharePoint servers enables scanning for file entitlement and classification of sensitive data which may be related to regulatory laws (e.g., GDPR, HIPAA).

NAS or network-attached storage is a file-level storage system based on networked appliances containing multiple storage devices. SharePoint is a web-based collaborating platform and a document management and storage system.

This Guardium product includes a Windows-based service performing scheduled scans of either NAS or SharePoint, and a configuration application for configuring the scan's targets, schedule, and classification criteria. This client software can be seen in S-TAP Control and the scan results are in the File Entitlement report.

- [\*\*Supported platforms for file discovery\*\*](#)
- [\*\*Scan Permissions\*\*](#)  
NAS and SharePoint permissions for File Discovery, Entitlement and Classification (FDEC)
- [\*\*Installing client software\*\*](#)  
Install File Discovery, Entitlement and Classification (FDEC) for your NAS or SharePoint environment.
- [\*\*Configure Scan Settings\*\*](#)  
Launch the Scan Configuration Utility using **ConfigurationFDEC.exe** in the installation directory under Bin\|. The configuration utility executable is the same for both NAS and SharePoint environments.
- [\*\*View Scan Results\*\*](#)  
View File Discovery, Entitlement and Classification (FDEC) scan results.
- [\*\*Creating User-Defined Criteria\*\*](#)  
The Criteria Editor is a utility that allows users to create criteria from scratch or by copying and editing a pre-defined criteria item.

---

## Supported platforms for file discovery

For the list of supported platforms for files, see [Guardium Supported Platforms for Files](#).

---

## Scan Permissions

NAS and SharePoint permissions for File Discovery, Entitlement and Classification (FDEC)

---

### SharePoint Scan Permissions

The SharePoint Agent is capable of auditing permissions and content, or Access Auditing (SPAA) and Sensitive Data Discovery Auditing, on SharePoint servers. It is installed on the application server which hosts the *Central Administration* component.

If limited provisioning of the service account is not required by the organization, then the following permissions are sufficient for successful SharePoint Agent-based scans:

- Local Administrator group membership on the on server where the SharePoint Agent is installed
- Site Collection Administrator on all Site Collections to be scanned
- DB\_Owner or SPDataAccess should be applied on the desired Configuration database and all Content databases depending on the SharePoint version:
  - For SharePoint 2013 and 2016: SPDataAccess on the SharePoint Content database and all Configuration databases
  - For SharePoint 2010: DB\_Owner on the SharePoint Content database and all Configuration databases

#### SharePoint Scan Permissions: Less Privileged Model

If restricted permissions are desired by the organization, the following permissions are needed for the service account to successfully run SharePoint Agent-based scans.

Prior to installation of the SharePoint Agent, the service account to be supplied during installation and later used to run the Access Auditing (SPAA) and/or Sensitive Data Discovery Auditing scans against the targeted SharePoint environment needs the following permissions:

- Log on as a Service in the Local Security Policy
- Local group membership to IIS\_IUSRS
- Performance Log Users (For Sensitive Data Discovery Only)

After the SharePoint Agent installation, this service account needs the following additional permissions to run the Access Auditing (SPAA) and/or Sensitive Data Discovery Auditing scans:

- Site Collection Administrator on all Site Collections to be scanned
- Local 'Users' group membership on server where the SharePoint Agent is installed

If the scans will include Web Application scoping, then the following permissions are also needed (this can be skipped if running full farm scans):

- Local group membership to Backup Operators
- Local group membership to WSS\_WPG
- WSS\_CONTENT\_APPLICATION\_POOLS on the SharePoint Configuration database

After the FDEC SharePoint Agent is installed, ensure that the service account has the following permissions:

- Full Control on the agent install directory, for example C:\Program Files\IBM\FDECforSP

The FDEC SharePoint Agent utilizes Microsoft APIs. The Microsoft APIs require an account with the following permissions in order to collect all of the data:

- WSS\_CONTENT\_APPLICATION\_POOLS on the SharePoint Content database(s)
- WSS\_CONTENT\_APPLICATION\_POOLS on the SharePoint Configuration database

If scans will include Web Application scoping, this last permission will already have been met.

## NAS Scan Permissions

### NetApp Data ONTAP Cluster-Mode Permissions

The credential used to collect file system data from a NetApp Data ONTAP Cluster-Mode device must have the ability to:

- Enumerate shares by executing specific API calls
- Bypass NTFS security to read the entire folder structure to be scanned and collect file/folder permissions

#### Share Enumeration – API Calls (Cluster-Mode)

To enumerate the shares on a NetApp Data ONTAP Cluster-Mode device, File System scans require a credential provisioned with the following CLI commands at minimum.

| CLI Command                     | Access   |
|---------------------------------|----------|
| version                         | Readonly |
| volume                          | Readonly |
| vserver                         | Readonly |
| server fpolicy                  | Readonly |
| security login role show-ontapi | Readonly |

Important: In order to enumerate shares on NetApp Data ONTAP Cluster-Mode device v8.3+, the credential needs to have at least the following permission on the target host: Group membership in the Power Users group.

#### Bypass NTFS Security (Cluster-Mode)

It is possible to enable a credential to bypass NTFS security on NetApp Data ONTAP Cluster-Mode devices by provisioning access to a special share: ONTAP\_Admin\$. In order to access the ONTAP\_Admin\$ share, the credential must be associated with an FPolicy on the target device.

The FPolicy can be an “empty” FPolicy and should have minimal impact on an organization’s system. The policy name must be “StealthAUDIT”.

### NetApp Data ONTAP 7-Mode Permissions

The credential used to collect file system data from a NetApp Data ONTAP 7-Mode device must have the ability to:

- Enumerate shares by executing specific API calls
- Bypass NTFS security to read the entire folder structure to be scanned and collect file/folder permissions

The following sections outline the required permissions granted to the credential used within the assigned Connection Profile for these target hosts.

#### Share Enumeration – API Calls (7-Mode)

To enumerate the shares on a NetApp Data ONTAP 7-Mode device, File System scans require a credential provisioned with access to (at minimum) the following API calls:

- login-http-admin
- api-system-api-list
- api-system-get-version
- api-cifs-share-list-iter-\*

#### Bypass NTFS Security (7-Mode)

In order to bypass NTFS, the credential needs to at least have the following permissions on the target host:

- Group membership in both of the following groups:
  - Power Users
  - Backup Operators

Note: All NetApp groups are assigned an RID. Built-in NetApp groups such as Power Users and Backup Operators are assigned specific RID values. On 7-Mode NetApp devices, system access checks for a group are identified by the RID assigned to the group and not by the role it has. Therefore, the ability to bypass access checks with the Power Users and Backup Operators group has nothing to do with the power role or the backup role. Neither role is required. For example, the built-in Power User group, even when stripped off all roles, still has more file system access capabilities than any other non-built-in group.

### EMC Celerra, VNX, VNxe, VMAX3, or Unity Permissions

The credential used to collect file system data from an EMC Celerra, VNX, VNxe,VMAX3, or Unity device needs to at least have the following permissions on the target host:

- Group membership in both of the following groups:
  - Power Users
  - Backup Operators

These permissions grant the credential the ability to enumerate shares, access the remote registry, and bypass NTFS security on folders.

If there are folders to which the credential is denied access, it is likely that the Backup Operators group does not have the “Back up files and directories” right. In that case, it is necessary to assign additional “Back up files and directories” right to those groups or to create a new local group, using Computer Management from a Windows server. Then assign rights to it using the CelerraManagementTool.msc plugin which is available to EMC customers.

Note: In order to successfully scan EMC devices from a Windows Server 2012 or newer, the “Require Secure Negotiate” policy must be turned off on that server. This is due to a problem that is caused by the “Secure Negotiate” feature which was added to SMB 3.0 for Windows Server 2012 and Windows 8. This feature depends upon the correct signing of error responses by all SMBv2 servers, including servers that support only protocol versions 2.0 and 2.1. Some third-party file servers do not return a signed error response; therefore, the connection fails.

### EMC Isilon Permissions

The credential used to collect file system data from an EMC Isilon device must have the following permissions on the target host:

- Group membership in the local Administrators group – LOCAL:System Provider
- Rights on the actual file tree or to the IFS root share
  - Share Permissions
    - Read access
  - Folder Permissions
    - List Folder / Read Data

- Traverse Folder / Execute File
- Read Permissions

These permissions grant the credential the ability to audit folders and shares. In order to execute scoped Classification scans, the credential must also have the LOCAL\System provider selected in each access zone in which the shares to be scanned reside.

#### Hitachi Permissions

The credential used to collect file system data from a Hitachi device must have the following permission on the target host:

- Group membership in both of the following local groups:
  - Local Administrators
  - Backup Administrators

This permission grants the credential read access to all target folders and files.

## Installing client software

Install File Discovery, Entitlement and Classification (FDEC) for your NAS or SharePoint environment.

### Before you begin

- Users must have matching administrative privileges on both the server side as well as NAS and SharePoint environments. For more information, see [Scan Permissions](#).
- For detailed platform prerequisites and support for NAS devices, see [Supported platforms for file discovery](#).

### Procedure

1. Determine what environment to use. If you want to install the client to scan a NAS device, install the client on a Windows server that can access the NAS device through the network. But if a user wants to install the client to scan SharePoint, install it directly on the SharePoint server or SharePoint server farm.  
Note: Do not install any other Guardium products on this server.
2. Download the FDEC for NAS and SharePoint package to the server from [Fix Central](#) and extract the file.  
Note: Before you extract the file, it is recommended that you can unblock the compressed file that is downloaded to the server. To unblock the compressed file:
  - a. Browse the file in your server, right-click on the file, and select Properties.
  - b. Select Unblock, and save your changes
 If the file is already unblocked, then the Unblock option is not available.
3. Go to the FDEC package installer directory and run the executable file **setup.exe** in the installer directory.  
The default installation directory for FDEC for NAS is C:\Program Files\IBM\FDECforNAS.  
The default installation directory for FDEC for SharePoint is C:\Program Files\IBM\FDECforSP.
4. Follow the prompts in the wizard to complete the installation.
  - a. Specify the service user who has admin privileges for the share they want to scan.
  - b. In the Network Addresses page, enter a list of Guardium hostnames or IP addresses. If there is a failover, the FDEC agent connects to the next appliance on the list.

## Configure Scan Settings

Launch the Scan Configuration Utility using **ConfigurationFDEC.exe** in the installation directory under Bin\|. The configuration utility executable is the same for both NAS and SharePoint environments.

Use the following options to configure the scan settings:

| Scan configuration | Description                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scan Name          | An arbitrary name for your scan.                                                                                                                                                                                                                                                                                                                                                   |
| Guardium Appliance | The hostname or IP address of your Guardium Appliance.<br>In a NAS environment, scans can run concurrently, and each scan can be configured with a different appliance address.<br>Click Manage to enter a list of Guardium® appliances. You can test the connection on each appliance individually. In the event of a failover, the agent connects to the next appliance on list. |
| Local Host Address | The IP address of the local host.                                                                                                                                                                                                                                                                                                                                                  |
| Scan Host          | For NAS, this is the IP or hostname of NAS environment.<br>For SharePoint, Scan Host is auto-filled with localhost.                                                                                                                                                                                                                                                                |

| Scan configuration                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scan Paths                           | <p>Here are some examples of scan paths:</p> <ul style="list-style-type: none"> <li>For NAS: NameOfShareDrive</li> </ul> <p>Notes:</p> <ul style="list-style-type: none"> <li>The NameOfShareDrive supports the share, zone, or drive name. However, you cannot specify the path.</li> <li>To make scanning time of the whole NAS device more manageable, you can split it into smaller shares, and create a scan for each share.</li> </ul> <ul style="list-style-type: none"> <li>For SharePoint: http://SharePointServer/my/test</li> </ul> <p>Click  to select, add, or remove site collections to the scan. To create a farm-wide scan, do not specify a path.</p> <ul style="list-style-type: none"> <li></li> </ul> |
| Scan Every                           | <p>The scan schedule can be configured in hours or days. By default, the frequency of the scan is every 12 hours.</p> <p>Scans can also be scheduled to run at a specific time.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Run Now                              | <p>Use this option to run a scheduled scan immediately.</p> <p>To activate the Run Now button, click </p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Directory Level                      | The number of levels that will be scanned in the directory structure. The default is 100                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Scan Options                         | <ul style="list-style-type: none"> <li>Containers Only: scans only directories, and will not trigger classification on the objects themselves.</li> <li>All Objects: scans everything including files, directory tree, and will match criteria.</li> <li>Matches Only: this scan only returns records that trigger criteria.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                    |
| Scan Criteria                        | <p>This allows for upload of various criteria sets. You may select the specific criteria you wish to use for classifying files. As an example: GDPR sensitive data patterns can be selected from the GDPR.update file. For criteria that align with other compliance guidelines such as HIPAA, select patterndefs.update.</p> <p>To create user-defined criteria, see <a href="#">Creating User-Defined Criteria</a>.</p>                                                                                                                                                                                                                                                                                                  |
| Scan Service Account                 | <p>The service account for each scan can be configured independently to reflect the environment being scanned.</p> <p>After you save a scan, click  to activate the scan.</p> <p>Click  to stop a scan.</p> <p>Click  to restart a scan.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| New Scan, Save Scan, and Delete Scan | <p>Use these buttons to create, save, or delete a scan.</p> <p>You must click the  button to activate a scan after it is saved.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Purge scan DB                        | Purge your local database periodically for fresh scan results. You must also purge the local database in the event that a scan is interrupted.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Scan Status                          | This displays the scan status including Started Last Scan, Finished Last Scan, Scanned Objects, New and Updated Objects, Deleted or Renamed Objects.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

Note:

- After you configure and save the scan, click to activate the scan.
- Scans can be scheduled to run concurrently. But if two scans target the same host, they will run consecutively.
- The default maximum size for file classification is 2MB.

#### Notes on Upgrading:

It is not recommended to upgrade the scan configuration utility until the scan is finished. Upgrading or stopping the service may corrupt the scan results.

When you upgrade your scan utility, you must reenter the service account credentials. During the upgrade, all active scans will have new services created for them, and they will begin running according to their schedule. You must click the play button to enable all new, and inactive scans.

---

## View Scan Results

View File Discovery, Entitlement and Classification (FDEC) scan results.

### About this task

Before you run the scan, check to see if the agent is connected to the appliance. The scan results can be viewed through the File Entitlement and Directory Entitlement reports on My Dashboard.

### Procedure

- Click My Dashboards > Create New Dashboard to open a new dashboard.
- Click Add Report to display a list of available reports. The Add a Report dialog shows a list of all reports that meet your criteria. You can browse the list of reports or type a string in the Filter field. The list of reports is updated as you type.
- The scan results can be viewed through the File Entitlement and Directory Entitlement reports. Click on the report to add it to your dashboard.

## Results

---

You now have a dashboard that gives you easy access to the File Entitlement and Directory Entitlement reports.

## Creating User-Defined Criteria

The Criteria Editor is a utility that allows users to create criteria from scratch or by copying and editing a pre-defined criteria item.

The criteria editor can be launched from **DLPCriteriaEditor.exe** in the installation directory under Bin\SensitiveData.

To create a new criterion from scratch, click the "+" button and select the criteria type. Provide the needed information for the selected criteria.

To change a pre-defined criterion, right-click the desired System Criteria list and select Copy. A copy of the selected criteria list will appear under My Criteria with *copy* added to the name. The copy can then be edited as desired.

There are three types of criteria to choose from:

- Regular Expression Criteria
- Keywords Criteria
- Summary Criteria

Two items are included as part of all three criteria types:

1. The Title appearing under My Criteria should be unique and descriptive.
2. The Only for use in Summaries checkbox causes the criteria to be used only as part of the summary criteria.

### Regular Expression Criteria

Regular Expression criteria are a set of pattern-matching rules that provide a concise and flexible means for matching strings of text. This criteria type can be used to verify a series of numbers as potentially valid, e.g. credit card numbers.

- The Case Sensitive checkbox causes the scan to be case sensitive.
- The Use validation checkbox allows for Luhn or Mod 11 validation.
- The Analyze checkboxes allow criteria to be built to analyze Filename, File Metadata, and File Content.
- The textbox is where the expression is entered.
- The Number Slider indicates the number of matches from the list needed to classify a file as potentially sensitive.

### Keywords Criteria

Keywords criteria consist of a list of comma-separated words. If any word in the list is found in the file, it is considered a hit.

- If checked, the Case Sensitive checkbox causes the scan to be case sensitive.
- The Analyze checkboxes allow criteria to be built to analyze Filename, File Metadata and File Content.
- The textbox is where the keywords are entered.
- The A..z button will sort keywords alphabetically and automatically remove duplicates. If checked, the Distinct checkbox causes the scan to search for unique hits of criteria.
- The Number Slider indicates the number of keywords from the list needed to classify a file as potentially sensitive. If Distinct is checked, this is the number of unique keywords needed.

### Summary Criteria

Summary Criteria are designed as a way of combining Regular Expression Criteria and Keywords Criteria for reporting purposes. These results are calculated according to the selected comparison operator (Any of, All of, or At least, which uses the value of the Number Slider).

- Check the desired criteria from My Criteria, System Criteria, or both.
- A *Summary Query* statement builds at the bottom with the appropriate comparison operator.

Select the radio button for the desired comparison operator. If At least is selected, a Number Slider appears to set the minimum number of criteria matches.

---

## Entitlement Optimization

Entitlement Optimization mediates between the role of the DBA in providing users the entitlements that are required to perform their jobs efficiently, and the role of Security in keeping entitlements as accurate and as minimal as possible to prevent system vulnerabilities.

Situations naturally arise during day to day management of the system that result in vulnerabilities, for example:

- Over-generalized access
- A privilege that was given to a user needed for one-time use but not removed afterward
- Changes over time of users and tables, resulting in dormant users and tables
- Privileges that are passed from one user to another

Entitlements require constant ongoing vigilance. For example, advanced persistent threats (APT) usually originate with one of these back door entries into the system.

Entitlement optimization constantly analyzes users' privileges and actions, and produces recommendations that pinpoint specific actions that aim to minimize user access to only that which is required. The analysis is entirely performed by the system. The admin reviews the results, examines each case, and takes the appropriate actions, for example, removing privileges from a DB user, or deleting dormant roles.

You can also investigate entitlement changes over the past week, a complete list of users and roles, data source privileges alongside their actual usage, and a simulated justification of a specific user-role combination. These views provide information relevant to the recommendations, and are also starting points for other investigations.

The advantages of entitlement optimization over Guardium reports is that it consolidates information for all database types (that appears in multiple Guardium reports), and it adds new analyses into its own comprehensive and consolidated reports, simplifying entitlement management, and thereby increasing system security.

Entitlement optimization supports database types: Microsoft SQL Server, Oracle. It does not support SQL Contained Databases. (Guardium reports are per database type.)

Entitlement optimization activity monitoring is limited to the data currently monitored by Guardium. The accuracy of the Recommendations, Entitlement browse and What if analyses depend on the relevance of the monitored data. To fully maximize the potential of this tool, configure the userScope and objectScope parameters, and consider modifying the security policy.

Users that are dormant from the time you start monitoring with Entitlement optimization are not included in the entitlement optimization reports. To watch a specific user that is monitored but doesn't have any recommendations, manually check the activity of the user either through entitlement browse or any of the other Guardium activity monitoring tools. The tools have the full information if the policy is correctly defined.

Entitlements analysis is per Collector, and operates only on the data sources that you configure by grdapi.

The **must gather** feature supports entitlement optimization. See [Basic information for IBM Support](#).

Access entitlement optimization from Discover > Database Entitlements > Entitlement Optimization

- [Enable and configure entitlement optimization](#)  
Use GuardAPI commands to enable and configure entitlement optimization.
- [Entitlement Optimization What's New](#)  
The What's New tab summarizes the additions and changes that are made to the system over the calendar week, from Sunday to Sunday.
- [Entitlement Optimization Users and Roles](#)  
The Users and Roles tab lists all users and their roles for all data sources that are enabled for Entitlement Optimization on this collector.
- [Entitlement Optimization Recommendations](#)  
Recommendations pinpoint specific actions that aim to minimize user access to only that which is required.
- [Entitlement Optimization Browse entitlements](#)  
Use the views and filters in this window to see the activity level of entitlements, and the lineage of the entitlements.
- [Entitlement Optimization What If](#)  
What If shows the probable justification for entitlement of a specific user with one or more specific verbs on a specific object (regardless of whether or not the entitlement exists).

## Enable and configure entitlement optimization

Use GuardAPI commands to enable and configure entitlement optimization.

All commands are run on the collector, and use already defined Guardium data sources. First, enable the feature on the collector, and then specify the data sources and enable the specific features.

The most accurate results are obtained by fine-tuning the data that is included in the entitlement optimization.

Users and Roles, and Browse entitlements, are enabled by default, however you must set extractActivity and extractEntitlement to `true` to extract the relevant data. The other three features (What's New, Recommendations, What If) are enabled individually. For example, you can enable Recommendations while leaving What If disabled.

Entitlement recommendations uses a subset of data, filtered by the userScope and objectScope parameters. Browse Entitlements uses the userScope parameter to filter data. Both parameters specify one or more Guardium® groups. Most likely, you will create specific groups to use for this purpose. Define the groups to extract only the data you want, to minimize storage and processing. The groups should have Full Audit, so that all data is analyzed and the results are conclusive. When you use groups with Full audit, the Browse Entitlements shows all rights of all users, regardless of their activity. A user that is outside of the userScope definition appears in the window, but its activity count is "unknown."

The best practice is to carefully evaluate and design your data collection scheme such that you only rarely change it. This is for two reasons: every time you change the configuration, it takes a week to generate data for reports; the data is compared to data of the previous 3 weeks, and when you change the data definition the comparison is less meaningful for the first 3 weeks.

Data is present in each tab from the first Sunday after you enable the individual feature.

For more information about the entitlement optimization functions, see [Entitlement optimization APIs](#).

Prerequisites

- Investigation dashboard is enabled. (Required for What-if, Recommendations, and updating activity in Entitlement Browse.)
- The user that configures the entitlement optimization must have permission to all the meta data and schema tables that are in the configured datasources.

## Related reference

- [Entitlement optimization APIs](#)

## Entitlement Optimization What's New

The What's New tab summarizes the additions and changes that are made to the system over the calendar week, from Sunday to Sunday.

Data is presented in the tab from the first Sunday after you enabled the feature.

The What's New tab presents:

- The number of new Users, Roles, Objects, and the number of databases associated with these additions
- The number of new Grantees and Grantors and the number of grants

### What to look for

Look for current trends, for example, by drilling-down to find:

- Unusual type or quantity of changes in the entitlements
- Most active grantors / grantees

Click Details in any topic to open a detailed table of the additions. For example, the details on new users are the server and service name.

## Entitlement Optimization Users and Roles

The Users and Roles tab lists all users and their roles for all data sources that are enabled for Entitlement Optimization on this collector.

Data is presented in the tab from the first Sunday after you enabled the feature.

This tab is based on the standard Guardium user and roles report that presents data on only one database type. It presents:

- Host
- Service Name
- DB type
- Grantee
- Grantee type
- Role

You can use the standard Query-Report Builder functions, which are accessed by the icons above the table.

## Entitlement Optimization Recommendations

Recommendations pinpoint specific actions that aim to minimize user access to only that which is required.

Data is presented in the tab from the first Sunday after you enabled the feature.

The system is continuously evaluating users and privileges. The weekly Entitlement recommendations report is based on the last 3 weeks of data (by default), such that each new report overlaps with data of the previous report. The Recommendations tab is equivalent to the Recommendations report in "Reports", which can be enabled as a distributed report.

If you customized the userScope parameter, the recommendations only include users from the specified user groups. The userScope and objectScope parameters are used in order to explicitly define the scope of recommendations. In order to maximize the accuracy of recommendations regarding users and objects, the users and objects in the specified groups should have Full Audit.

All recommendations must be thoroughly investigated by the admin, by drilling-down for specific server, database, object, and recommendation type, before implementation.

The top of the tab contains a pie graph that shows the recommendations by type. The table at the bottom of the window lists the recommendations. You can modify the recommendations report using the standard reports icons, export the report by clicking Export, and map to API by clicking Actions.

The recommendations types are:

Table 1. Recommendation Types

| Type                         | String                                                                        | Details                                                                                                                                                                                                                                                                                                                                |
|------------------------------|-------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ANOMAL USER                  | User {object} has anomalous activity within role {source}                     | User activity count within a specific role is anomalous. This means the user is either much more active or much less active than other users.                                                                                                                                                                                          |
| ALERT ACTIVITY (Ad-hoc user) | User {source} used the privilege {verb}-{object} but no entitlement was found | A typical ad hoc user gives itself permission, performs an action, and then removes the permission. Users can be erroneously identified as ad hoc due to the time differences between the entitlement changes and their activities. Use the Guardium Activity Monitoring Tools to determine whether or not the privilege is justified. |
| DORMANT_USE_R                | Remove inactive or empty user{object}                                         | User has no assigned privilege or had no activity within the given interval.                                                                                                                                                                                                                                                           |
| DORMANT_ROLE                 | Remove inactive or empty role{role}                                           | No users, no activity by any users, or empty privileges                                                                                                                                                                                                                                                                                |
| REVOKE_FROM_USER             | Revoke{verb}-{object} from user {source}                                      | User did not perform any activity on the relevant object, verb.                                                                                                                                                                                                                                                                        |
| REVOKE_FROM_ROLE             | Revoke{verb}-{object} from role {source}                                      | ALL the users within the specific role didn't perform any activity on object, verb.                                                                                                                                                                                                                                                    |
| REMOVE_FROM_ROLE             | Remove user{object} from role{source}                                         | User didn't use any of the privileges granted to him by the role.                                                                                                                                                                                                                                                                      |
| INACTIVE DATABASE            | Database has no activity                                                      | If the unused database cannot be justified, remove it.                                                                                                                                                                                                                                                                                 |

## Entitlement Optimization Browse entitlements

Use the views and filters in this window to see the activity level of entitlements, and the lineage of the entitlements.

Data is presented in the tab from the first Sunday after you enabled the feature. After the first Sunday, the activities are updated daily.

This information is useful for general entitlement investigation, and to further evaluate recommendations in the Recommendations report. The default view in this window is a bar chart of the datasources with the highest rates of unused privileges.

Entitlement browse shows all the entitlements of the data sources defined in the grdAPI that have extractEntitlement available. This is true if the activity collection is off, and if the user scope and object scopes are defined. You can always search and see the permissions of all the users.

The activity count field results are affected by the userScope parameter, as follows:

- Users that are included in the userScope:
  - Active users appear green and have numerical results in the activity count column
  - Non-active users appear red and the activity count is "Not active"
- Users that are not included in the userScope:
  - Active users appear green and have numerical results in the activity count
  - Non-active users appear gray and the activity count is "unknown"

Typical investigations are:

- Determine which objects a user has permissions for and whether he uses them
- Determine whether a user utilized his permission on an object at the specific time it was permitted
- Are there permissions that are used more than expected?
- Are there permissions that are used only once?
- What is the lineage of the permissions that have been unusually utilized: explicit, or implicit, inherited from a parent role, or role hierarchy?

To get more details on how a specific privilege is used, with full SQL, you can search for Data Activity (Investigate > Search for Data Activity), right-click the DB User or Source program in the Results Table, and select Full SQL by DB User.

Unused entitlements are typically one of:

- Action rarely performed, but a valid entitlement, for example generating a quarterly report
- Unused and therefore not justified (point of vulnerability)

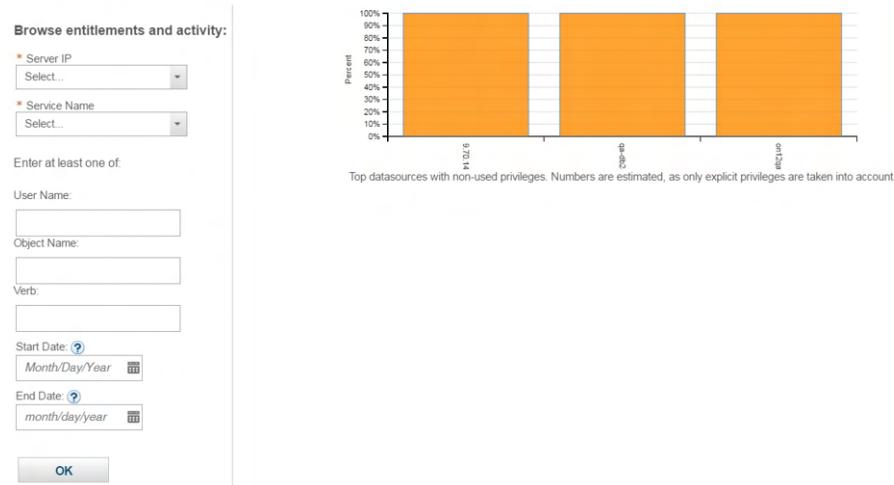
To view entitlement usage on a specific service on a specific server:

1. On the left side, select a server IP and service.
2. Filter by one or more of: Name, Object Name.
3. Optionally enter a Verb or date range.

Figure 1. Selecting entitlement criteria

To explore entitlement breakdown in a datasource instance, specify either user, object, or verb. The default bar chart shows Top datasources with non-used privileges.

Data shown may be incomplete due to data collection policy.



The table presents the Grantee type, Grantee, Verb, Name, Activity count, and Lineage. A user can have multiple privilege lineages: explicit, or implicit, inherited from a parent role, or role hierarchy.

## Entitlement Optimization What If

What If shows the probable justification for entitlement of a specific user with one or more specific verbs on a specific object (regardless of whether or not the entitlement exists).

Data is available in this tab from the first Sunday after you enabled the feature.

Guardium analyzes the behavior of similar users to produce the probable justification, which is some cases provides highly relevant information. The analysis can be useful when you examine unused entitlements, and the REVOKE\_FROM\_USER recommendation. It is a general indication, and should be used together with other entitlement optimization functions.

Enter these details and click OK to generate the probability:

- User name
- Object name
- Verb (one or more)
- Server IP

- Service name

Possible responses are:

- The probability that this DB user will use this privilege is **n%**. Probability of 100% indicates that the user used the activity at least once.
- Failed to find data source on server.
- Object and DB user are not in scope.
- No sufficient evidence found for DB user and privilege: either the User / Object / Verb does not exist in the selected database, or no activity is found for the user, or no activity has been found for the object, verb tuple. Possible fixes: wait for activity collection to run; make sure the input is entered correctly.

## Protect

After you identify databases and file systems that contain sensitive data, you can take several steps to protect that data. Protection options include masking data, alerting personnel based on data access, and establishing policies that enforce access restrictions.

- **[Active Threat Analytics](#)**  
The Active Threat Analytics dashboard shows potential security breach cases, based on the outlier mining process and on identified attack symptoms. In this dashboard, you can view and investigate cases, and take actions on individual cases.
- **[Risk Spotter](#)**  
Risk Spotter is a First of its Kind technology, changing the security paradigm to an Artificial Intelligence Data Protection Policy. It uses a holistic algorithm to dynamically assess risk factors, and it uses a smart algorithm to identify potential risks across your entire system.
- **[Outliers detection](#)**  
Enable and start auditing outlier detection in two easy steps, letting Guardium do the work of identifying abnormal server and user behavior, and providing early detection of possible attacks.
- **[Real-time trust evaluator](#)**  
The Real-time Trust Evaluator (RTTE) evaluates the application connections that are monitored by Guardium®. Connections are classified as "untrusted", "evaluated" or "trusted". Trust scores (value from 0 - 100) are assigned to each classified connection. Connections that are not classified as trusted or untrusted are classified as evaluated.
- **[Policies](#)**  
Policies are sets of rules and actions applied in real time to the database traffic observed by a Guardium system. Policies define which traffic is ignored or logged, which activities require more granular logging, and which activities should trigger an alert or block access to the database.
- **[Managing correlation alerts](#)**  
An alert is a message that indicates that an exception or policy rule violation was detected. Create and manage correlation alerts from the Add Alert page.
- **[Incident Management](#)**  
The Integrated Incident Management (IIM) application provides a business-user interface with workflow automation for tracking and resolving database security incidents.
- **[How to manage the review of multiple database security incidents](#)**  
Incident management - track and resolve database security incidents.
- **[Query rewrite](#)**  
Query rewrite functionality provides fine-grained access control for databases by intercepting database queries and rewriting them based on criteria defined in security policies.
- **[File Activity policies for UNIX and Windows file servers](#)**  
File activity policies are used to protect sensitive data on UNIX file servers, Windows file servers,
- **[File activity policies for network-attached storage \(NAS\) and SharePoint](#)**  
Set up file activity monitoring for NAS devices and SharePoint by defining policies and rules in the Policy Builder for Files.
- **[Configuring consolidation of FAM MS Office events](#)**  
Use the FAM monitor Office event consolidation feature to filter out the extraneous, irrelevant MS Word, Excel, and PowerPoint file activities.

## Active Threat Analytics

The Active Threat Analytics dashboard shows potential security breach cases, based on the outlier mining process and on identified attack symptoms. In this dashboard, you can view and investigate cases, and take actions on individual cases.

Active Threat Analytics runs on central managers and stand-alone units.

Prerequisite: Threat finder and DAM Outlier mining are enabled. Click the Active Threat Analytics Setup link to enable Threat finder and DAM Outlier mining. Active Threat Analytics shows results for all collectors on which DAM Outlier mining is enabled.

Access Active Threat Analytics from the Welcome page or from Protect > Uncover threat vectors > Active Threat Analytics.

The first row of results tabulates all cases and all open cases per: databases, DB users or OS users, file systems and file user. The cases in each category are identified by their risk level: high, medium, and low. If a database, database user, file system, or OS user is associated with multiple cases, that database or user is only counted one time.

For example, assume there are 40 cases. 10 of which are associated with database NN, 10 of which are associated with user XX, and the remaining 20 associated with various databases or users. In this case, the total of database and file server cases and database and file user cases would be 22, and not 40.

By default, data is presented for the last day. You can change the time period from the drop-down list.

The table shows violations, outliers, errors, and activities over the same period of time.

The table lists all cases (in descending order of severity), including the type of threat, the observed activity on which the case is based, and the source details. Active Threat Analytics identifies potential security breaches by case type, listed in [Threat descriptions](#).

Click Databases, DB users, File Systems, and OS users to open a summary of the entities with open cases. From there, you can click View Profile to open the Behavioral Analytics for the specific database or user, and view all cases that are associated with this entity, the distribution of working hours, and the distribution of verbs. For database users, you can also click User Risk Indicators to open the Risk Details window, showing the Risk Spotter risk indicator scores.

Attention: Each high severity case is a suspected threat that should be investigated immediately. High severity cases can also be caused by a patch installation. In this case, you would close the case. Low severity cases can be anomalies. If so, consider closing the case.

When you are investigating cases:

- Get a clear picture of whether this is an isolated incident, or one of many on the source.
- Change the time frame or filters for a narrower or broader cross section, and look for patterns or other unusual behavior.
- Look at the distribution of activity per verb, distribution over time, average activities, errors, and so on.
- For database users, look at the risk score and analysis.

In the Cases table, you can:

- Click the  next to the case number to open the Case Analysis page, giving a detailed analysis of the case from a few perspectives. This is the starting point of your investigation:
    - Case details: time, type, observations, details specific to the case type, and a link to the following reports.
      - SQL Report  
SQL statements with limited information.
      - Full SQL Report - Full SQL statements  
Available only if the Log full details rule action applies according to the installed policy. The default time period for the Full SQL report is one hour.  
When you are investigating cases, also look at shorter time periods, and earlier time periods.
      - SQL Exceptions Report  
SQL exceptions, including the SQL statement that caused the exception.
    - Source details: statistics and activities on the source, distribution of activities by time period, history of cases, and types that were opened (and closed) on this source.
    - Exploration: Five sets of tables that give context to this case, and provide a deep-dive into your investigation.
- Where  
More details on the server and database, for example, number of databases (and their types) on the server, number of cases of the same type seen on the database.
- When  
Time period details: work hours, off-work hours, weekends, what else happened during this time.
- What  
Details of similar cases: Case statistics, sensitive objects accessed (and by which commands), other occurrences of this case (and where).
- Who  
Statistics on the users that accessed the database, users that normally access this database (OS users, DB users), and from which client hosts. For OS users: the client hosts this user accesses from, and when it was first used (as recorded in Guardium).
- How  
Statistics on the applications used to access the database. Applications that were used during the case time window, applications that are normally used, First record of use of application (as recorded in Guardium).

You can also take actions on individual cases:

- Assign case: Assign the case to a role, an email, a user group, or a user. Roles and groups are preferable, since individual users and emails can change.
  - Add to group: Select either Server IP, database, DB user, file system, or file user and add it to either an existing group or a new group. This is useful for tracking users and activity. You can use these groups in policies, reports, and alerts for enhanced monitoring over your system.
  - Close case: If the observed behavior is acceptable, consider closing the case. Before you close the case, you can also assign the case a threat category and severity level based on your own input by completing the Actual threat category and Actual severity fields.
  - Add a comment.
  - Open case dashboard: Opens the Investigation Dashboard, filtered for the selected case. Drill down for details of symptoms, compare to other databases and users, and view activity over time. See [Investigation Dashboard](#).
  - Add items to an exclusion list. For more details, see [Excluding items from Active Threat Analytics](#).
- Filter the entire table by threat category by using the drop-down menu or the free text field.
  - Filter the entire table by severity level (high, medium, or low).
  - Filter the table to show either only unassigned cases only or only cases assigned to an audit process or an external ticketing system, such as ServiceNow.

The threat cases are not copied to the secondary central manager. In the case of a failover, there are no known threat cases in the new primary central manager.

- [Threat descriptions](#)  
Understand the different types of threats identified by Active threat analytics.
- [Creating threat categories from policy rules](#)  
You can use your policies' rules to create active threat analytics case types, by setting a threshold on specific violation policy rules.
- [Excluding items from Active Threat Analytics](#)  
Exclude items from the Active Threat Analytics process.
- [Active Threat Analytics setup](#)  
Enable and disable, and monitor, the active threat analytics processes, both across your entire system (recommended), or on individual managed units.

## Related concepts

- [Risk Spotter](#)
- [Investigation Dashboard](#)

## Related information

-  [Active Threat Analytics case analysis video](#)

## Threat descriptions

Understand the different types of threats identified by Active threat analytics.

#### Account takeover

A nonauthorized user accesses an account.

A case is opened when an account is accessed by a new connection profile. For example, a known user is connecting from a different source IP or is using a different source program. Errors or exceptions that are associated with the source are also reported.

#### Anomaly

Anomalies are behaviors that are contrary to "normal" behavior in any aspect of tracked activity.

Guardium® identifies anomalies by using outlier mining (including the volume of outliers, severity of individual events, and predicted volume of outliers at specific times of day), and an anomaly detection algorithm.

#### Brute force attack

Suspected failed login attacks cover many scenarios. The failed logins are usually by one database user or by multiple database users on one database. The factors that are considered include the user, the timing, the frequency, and other actions taken by the suspicious user.

#### Cross-site scripting

Cross-site scripting (XSS) attacks attempt to insert malicious JavaScript code into the server through client input fields and APIs. When such a script is in place, it is persistent and activated every time that a user accesses the affected page. A typical scenario inserts JavaScript through a web page and then runs every time that page is accessed.

Guardium constantly monitors for XSS patterns in database requests.

#### Data tampering

A data tampering attack attempts to change or delete information. This type of attack typically exhibits a high volume of data deletion or removal.

Guardium observes whether errors are generated by the data deletion and whether the removal or deletion actions affected sensitive data.

#### Denial of Service

A denial of service attack attempts to impact service availability by creating excessively high demands on memory or resources or by causing server unavailability.

One means of identifying these attacks is by a high volume of outliers and weighted anomalies. The volume of outliers in this case is high enough to impact availability: for example, a thousand times the average activity.

#### Insider threat: possible data leak

This attack is an attempt to retrieve data for unauthorized use.

Data leaks are identified by abnormally high data retrieval activity. The activity can be either the number of activities or the number of records that are affected, depending on whether records affected tracking is enabled in the Guardium environment.

#### Malicious stored procedure

A malicious stored procedure is a block of SQL code that is designed to evade detection and to run complex attacks over an extended time period. The stored procedure can be run repeatedly, change its behaviors over time, or remain dormant for long periods of time, all of which makes it harder to identify its activities as suspicious. For example, a stored procedure that caused unusual activity to be identified in an audit can go dormant and be forgotten by the time of the next audit. A malicious stored procedure can be used to disguise the drop of an important table or to extract the contents of a table. Examples of suspicious activity include:

- The creation of a stored procedure with a DROP statement that affects sensitive objects.
- SQL exceptions that are caused by missing objects.
- A procedure that is dormant for an extended time period but is then modified.

Guardium finds malicious stored procedures by tracking the activity around individual stored procedures and, together with outlier mining data, correlating the symptoms and users.

#### Massive grants

Symptoms of massive grant attacks include granting many new privileges to various users and permissions that are being granted by users that don't usually grant permissions.

Guardium identifies and flags such behaviors.

#### New grants

Granting privileges to users is a normal procedure. However, grants can also transfer privileges to users to stage attacks under a different username. Guardium opens a case if it identifies suspicious behavior of a user with recently granted privileges.

#### OS command injection

These attacks are attempts to run commands on the operating system, from a client to a process. For example, inserting operating system commands to erase files or, in Guardium, to set outlier mining parameters with the goal of preempting the identification of attack symptoms. The attacker usually does not know whether the attack succeeded and uses tools like ping to check communication between its client and the server.

Guardium observes patterns of operating system commands that an attacker might attempt to run on the target server.

#### Schema tampering

Schema tampering is characterized by changes to database elements such as tables, views, or stored procedures.

Guardium identifies these changes and correlates them with other factors such as whether the changes generated errors or were performed by a privileged user.

#### SQL injection (general)

SQL injection attacks attempt to exploit application vulnerabilities by concatenating user input with SQL queries. If successful, these attacks can run malicious SQL commands that use the legitimate application connection. SQL injection attacks can be difficult to identify because the individual steps of an attack, analyzed independently of the other steps, might be considered legitimate. Using threat detection analytics, Guardium identifies potential SQL injection attacks by capturing the individual steps and analyzing them as part of a single complex attack.

Typical symptoms of SQL injection attacks that Guardium identifies include:

- An attacker tries to identify the structure of a dynamic SQL query: for example, the number of columns queried.
- An unusually large quantity of new queries, specifically queries that are uniquely or unusually structured.
- Access to tables that contain information about the database structure.

#### SQL Injection: Tautology

In a tautology type attack, code is injected that uses the conditional operator OR and a query that evaluates to TRUE. Tautology-based SQL injection attacks usually bypass user authentication and extract data by inserting a tautology in the "WHERE" clause of an SQL query. The SQL query results transform the original condition into a tautology that causes, for example, all the rows in a database table to be open to an unauthorized user.

Guardium prevents this type of attack by identifying multiple variations on tautological expressions in the database requests.

#### SQL Injection: Side channel

SQL injection attacks often result in a general error with no indication of the reason for failure. In side channel attacks, the attacker typically inserts code that has a "side effect" like sleeping for 2 seconds if an attack is successful. This technique allows the attacker to measure the side effect and determine whether the attack was successful. For example, the injected code might sleep for 2 seconds if the MySQL version is 5.6: if the request takes more than 2 seconds to return, the attacker confirms that the server is running MySQL 5.6.

Guardium finds side channel attacks by identifying the use of commands such as sleep and comments in the database requests.

#### SQL Injection: Denial of Service

A denial of service attack attempts to impact service availability by creating excessively high demands on memory or resources or by causing server unavailability. Guardium identifies these attacks, for example, by analyzing the syntax used in the database requests.

# Creating threat categories from policy rules

You can use your policies' rules to create active threat analytics case types, by setting a threshold on specific violation policy rules.

## About this task

You can set thresholds on violation rules that have a severity of high in the rule definition, and the rule action is alert per match.

When the rule threshold is exceeded in any 1 hour, a case is created. The case type is the name of the rule. Cases that are created from a policy rule threshold appear in the active threat analytics cases table, and are treated like any other case.

Changes to installed policies are applied according to the policy schedule. When adding a threshold to a rule in an installed policy, cases are created for violations (according to the threshold) only after the policy is reinstalled.

Use the API to define thresholds on rules. You cannot define thresholds in the GUI.

## Procedure

1. Identify which policy and which rule you want to use. Use the API commands `list_policy` and `list_policy_rules`.
2. Add or modify the threshold by using the API command `add_threshold_to_rule` or `update_threshold_in_rule`. For example, to add the threshold 25 to ruleNNN in policyAAA:

```
grdapi add_threshold_to_rule policy_name=policyAAA rule_name=ruleNNN threshold=25
```

## Results

From the next day (after the policy has been updated), when the rule threshold is exceeded in a timeframe of one hour, a case is created.

## Related reference

- [add\\_threshold\\_to\\_rule](#)
- [list\\_policy](#)
- [list\\_policy\\_rules](#)
- [list\\_rules\\_with\\_threshold](#)
- [remove\\_threshold\\_from\\_rule](#)
- [update\\_threshold\\_in\\_rule](#)

# Excluding items from Active Threat Analytics

Exclude items from the Active Threat Analytics process.

## About this task

You might want to exclude certain sources and activities from the Active Threat Analytic processes altogether to optimize resources and reduce false positives. For example, test data or activities run by automated processes.

Excluding sources from Active Threat Analytics:

A source is a database, a database user (DB user), or an operation system user (OS user).

You can exclude sources from the analytics process based on the following attributes:

- Server IP
- Database
- Database user
- Operation system user

Each such row is called an exclude item, though it might match several sources. You can use the asterisk character as a wildcard that replaces any string. The sources are excluded from all Active Threat Analytic processes – Outlier mining, Threat finder, and Threat diagnostics.

Examples of exclude items:

Example 1  
Server IP=130.23.45.55

Result: all the databases on this server and all the DB users of these databases are excluded from analytics.

Example 2  
Server IP=130.23.\*

Database=QA\_\*

Result: all the databases that start with “QA\_” on all the servers in subnet 130.23 are excluded from analytics and all DB users of these databases are excluded as well.

Example 3

Database user=QATEST

Result: database user "QATEST" is excluded from analytics in all the databases

You can also choose to exclude sources only from a specific category. For example, to exclude a database only from the "New grants" category. The database is analyzed for all other categories.

Excluding activities from Outlier mining:

You can exclude activities and exceptions from the Outlier mining process only, based on the source program (application) or object. This capability can be used, for example, to exclude temporary tables or activities that are run by trustworthy applications to reduce false positives.

Excluding sources and activities from Active Threat Analytics on a temporary basis:

Specify start and end dates on the exclude item to exclude sources and activities temporarily.

Note: You can set dates in the future only and cannot use the exclude list to remove cases already created.

Restriction:

The following limitations affect only managed units that are working with Guardium versions that are earlier than 12.0, while their central manager is upgraded to version 12.0 or later:

- The managed unit is not updated when you update or delete an exclusion item.
- Items excluded temporarily, that is, items with an end date selected, do not take effect on the managed units.
- When you enter a future start date on an exclude item, the exclusion starts immediately on the managed units.
- Cases cannot be excluded based on their category when the cases are created from the managed unit.
- Cases that are created from the managed unit are not excluded based on their category.

## Procedure

1. You can view the exclude list as a whole from Active Threat Analytics setup. Go to **Manage > Maintenance > Active Threat Analytics Setup > Analytics exclusion section**, or click Active Threat Analytics setup from the main Active Threat Analytics page.
2. After you access the exclude list from either of these paths, you can edit the list by adding new items or removing existing items. To add an item, click the  icon and select a period start in the window that appears. You can then also select a period end, but it is not required. These 2 fields define the window of time that the case is excluded. (Step 3 addresses the other fields in this window). Remove an item by selecting it and clicking the  icon.  
You can also add new items to the exclude list (but not remove items or view or edit the exclude list as a whole) from some other places in the UI.
  - To add items to the exclude list from Active Threat Analytics, click Active Threat Analytics from the Welcome page or from **Protect > Uncover threat vectors > Active Threat Analytics**. Select a case whose source you want to exclude and click **Actions > Add to exclude list**. Or click  to view a case's details and then click **Actions > Add to exclude list**. Define the period start as usual.
  - To add items to the exclude list from the Investigation Dashboard, go to **Welcome > Investigation dashboard > Outliers tab**. In the Outliers table, right-click the wanted outlier and select **Add to analytic exclude list**. Define the period start as usual.
3. From all paths described thus far, you can view and adjust the exclusion parameters for an existing item. Select the case that you want to make edits for and click 
  - Add, remove, or edit the values for the fields in the window that appears. Define a Server IP, Database, Database user, and Operating system user to exclude in the respective fields (if relevant). Use an asterisk in these fields to mark things you want to ignore as a wildcard.
  - The Category field defines specific threat categories to exclude, and you can use it in tandem with the Server IP, Database, Database user, and Operating system user fields. You can read more about each threat category in [Threat descriptions](#).
  - If you do not want to see any cases from a specific category, you can deactivate the entire category. In the Categories section of Active threat Analytics setup, choose the categories that you want to deactivate and click **Actions > Inactivate**
  - The Source program and Object fields define specific activities and exceptions to exclude. These fields are only intended for cases that stem from the Outlier mining process only and they cannot be selected in tandem with the Category field.
  - Add a comment in the Comment field to remind yourself or other users why you are making the current exclusion selections.

## Active Threat Analytics setup

Enable and disable, and monitor, the active threat analytics processes, both across your entire system (recommended), or on individual managed units.

The Active threat analytics processes are the Threat finder and DAM outlier mining. Best practice is to enable all processes across all Guardium® systems. If required, you can enable processes selectively.

To open the Active Threat Analytics Setup, go to **Maintenance > Active Threat Analytics Setup**. There are three sections, each with a modules status.

### Enable all processes

Prerequisite for Threat finder: Quick search is enabled.

Click **Enable all processes** to enable Threat finder and DAM outlier mining on all managed units in your environment. The system responds with one message on the Threat finder status, and one message on the DAM outlier mining status.

### Enable threat finder

Prerequisite for Threat finder: Quick search is enabled.

Click **Enable** to enable Threat finder either on a central manager or stand-alone system. The system responds with a status message.

## Enable DAM outlier mining

---

When viewed on an aggregator this window presents details of the specific aggregator's collectors.

When viewed on a collector, only that collector is detailed.

To enable or disable outlier mining on all managed units in your environment: click **Enable All / Disable All**. To enable outlier on individual units: select them and click **Enable / Disable** from the Actions drop-down list. Best practice: Enable outlier mining for your entire environment. If you need to enable selectively, enable on aggregators in preference to collectors.

View the enable and disable history by clicking Outlier mining enable/disable history. Details include the collectors that send data to the aggregator, or if the collectors do not send data to the aggregator, and why not.

This table describes the DAM outlier mining section, and the recommended user actions.

| Column                                                                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                   | Actions                                                                                                                                                                                                                                          |
|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  Unit | Opens and closes the list of units that send data to this aggregator                                                                                                                                                                                                                                                                                                                                          | Click to view the list of units                                                                                                                                                                                                                  |
| Unit                                                                                   | Name of unit                                                                                                                                                                                                                                                                                                                                                                                                  | NA                                                                                                                                                                                                                                               |
| Unit type                                                                              | One of Collector, Aggregator, Central Manager                                                                                                                                                                                                                                                                                                                                                                 | NA                                                                                                                                                                                                                                               |
| Unit on/off                                                                            | Indicates whether the unit is on or off.                                                                                                                                                                                                                                                                                                                                                                      | NA                                                                                                                                                                                                                                               |
| Outlier Mining Enabled/Disabled                                                        | <ul style="list-style-type: none"><li>Aggregator: Indicates whether outlier mining on the aggregator is enabled.</li><li>Individual row of one collector or stand-alone unit: Green indicates that outlier mining is enabled locally.</li></ul> <p>Use the Actions drop-down menu to enable or disable outlier mining on the selected managed units.</p>                                                      | NA                                                                                                                                                                                                                                               |
| Anomaly Last Found                                                                     | The local date and time on the CM of the last outlier mining run that found one or more anomalies (outliers).                                                                                                                                                                                                                                                                                                 | NA                                                                                                                                                                                                                                               |
| Last Analysis                                                                          | The local date and time of the CM of the last outlier mining run (process end date and time).                                                                                                                                                                                                                                                                                                                 | NA                                                                                                                                                                                                                                               |
| Analysis Status                                                                        | <ul style="list-style-type: none"><li>One of:<ul style="list-style-type: none"><li>The status of the last outlier mining run.<ul style="list-style-type: none"><li>Green: the process ended successfully.</li><li>Orange: the process ended with warnings.</li><li>Red: the process ended with errors.</li></ul></li><li>The date and time when the initial learning is scheduled to end.</li></ul></li></ul> | If an error or warning occurred only once, wait for the process run again (next hour) and check the result. If an error repeats, contact technical support. For processes that did not end successfully, click Details to view more information. |
| Learning Since                                                                         | Date and time at which the outlier mining process was enabled. The process learns the resource's behavior since this time.                                                                                                                                                                                                                                                                                    | NA                                                                                                                                                                                                                                               |
| Quick Search on/off                                                                    | Indicates whether Quick Search and Solr are enabled on the managed unit. When Quick Search is disabled, this machine's data is not included in the Investigation Dashboard.                                                                                                                                                                                                                                   | See <a href="#">Enabling and disabling the Investigation Dashboard</a>                                                                                                                                                                           |
| Last Info. Update                                                                      | Last date and time the information in this row was updated. Data is usually updated in intervals of about 5 minutes.                                                                                                                                                                                                                                                                                          | NA                                                                                                                                                                                                                                               |
| Configured to Send Outlier Mining Data                                                 | Collectors only in multi-CM environment. Indicates whether a collector is configured to send data to an aggregator. (If not, either it is running outliers detection locally, or it's not configured to send data.)                                                                                                                                                                                           | NA                                                                                                                                                                                                                                               |
| Outliers data last received                                                            | Collectors only in multi-CM environment. Indicates when an aggregator last received data from collectors.                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                  |

## Predefined alert

---

There is a predefined alert Outlier Analysis Failure, that is triggered by failure of the outlier mining process. You need to configure it in the Alert Builder.

## Risk Spotter

---

Risk Spotter is a First of its Kind technology, changing the security paradigm to an Artificial Intelligence Data Protection Policy. It uses a holistic algorithm to dynamically assess risk factors, and it uses a smart algorithm to identify potential risks across your entire system.

- [Risk Spotter functions](#)  
Learn how Risk Spotter identifies risky users across your entire system.
- [Risk Spotter risk indicators](#)  
Guardium® applies the Risk Spotter algorithm to the audited data modules, to analyze multiple risk indicators and to calculate the overall risk scores of risky users.
- [Use the Risk Spotter results](#)  
The Risk Spotter page presents risk data over your entire system, with a few graphs and tables. Learn how to use the Risk Spotter data in your daily Guardium activities.
- [Create a Dynamic Auditing policy](#)  
Learn how to create and install a policy for Dynamic Auditing, to maximize your Risk Spotter results.
- [Configure and enable Risk Spotter](#)  
Configure and enable the required and optional Guardium and Risk Spotter modules, then enable Risk Spotter itself.

## Risk Spotter functions

Learn how Risk Spotter identifies risky users across your entire system.

Risk Spotter runs on central managers and on stand-alone systems. All collectors must be running V11.0 or later.

The Risk Spotter implements a dynamic risk assessment, considering multiple risk factors, including:

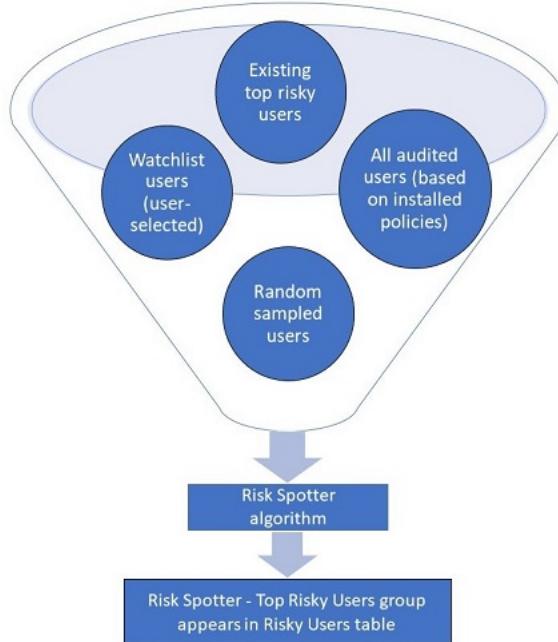
- Vulnerabilities and violations that are associated with the user
- Errors
- Threat Analytics findings
- Activity during off-work hours (defined by AFTER HOURS WORK and BEFORE HOURS WORK in the Time Period Builder page, and distributed from the central manager to its managed units.)
- Data access volume
- Volume of activities
- Access to sensitive data
- Type of commands the user ran (DML, DDL, SYSTEM, and so on)

The Risk Spotter algorithm uses Guardium modules to analyze the risk indicators and to identify risky users. Each user's risk overall risk score is calculated daily, based on the audited data. Risk Spotter assigns each user a score in the range 0 - 10. The detailed risk data is presented in the Risky Users table in the Risk Spotter page.

To maximize the Risk Spotter benefits, implement your own Risk Spotter Dynamic Auditing policy that uses the Risk Spotter - Audited Risky Users group. When you implement a Dynamic Auditing policy:

- Guardium® adds three types of users to the Risk Spotter - Audited Risky Users group, and audits the group continuously. The three types of users are:
  - Top risky users: Users identified by the Risk Spotter algorithm, together with your installed policies. Users in this group are carried over from day to day if their risk score warrants it. (The top risky users list is not copied to the secondary central manager. In the case of a failover, the Top risky users list is empty in the new primary central manager.)
  - Watchlist users: The Watchlist is a group of users that you populate, for further observation or investigation. You can add any user to the watchlist. These users remain in the Watchlist group in subsequent Risk Spotter daily iterations, regardless of their risk score.
  - Random sampled users: Risk Spotter continuously scans across your system, beyond your policy radar, evaluating non-audited users and identifying potential risky users.
- Risk Spotter updates the Risk Spotter - Audited Risky Users group members and reinstalls the policy during its daily process (1:00-2:00), effectively updating any policy that uses it.
- Guardium constantly monitors resources. If a managed unit's resources are overloaded for any reason, Guardium automatically uninstalls the Dynamic Auditing policy on the overloaded managed units. Uninstalling the policy does not impact the members of the Risk Spotter - Audited Risky Users group or Risk Spotter - Watchlist group. A user that is only audited by the Dynamic Auditing policy is not audited on the day the policy is uninstalled. New risky users on a collector that does not have the policy installed are not added to the Risk Spotter – Audited Risky Users group, and the risk score of existing users is not updated. Click Logs and Status to open the Risk Spotter events log to see which managed units do not have the policy installed.

Figure 1. Populating the top risky users group



## Related concepts

- [Active Threat Analytics](#)

## Risk Spotter risk indicators

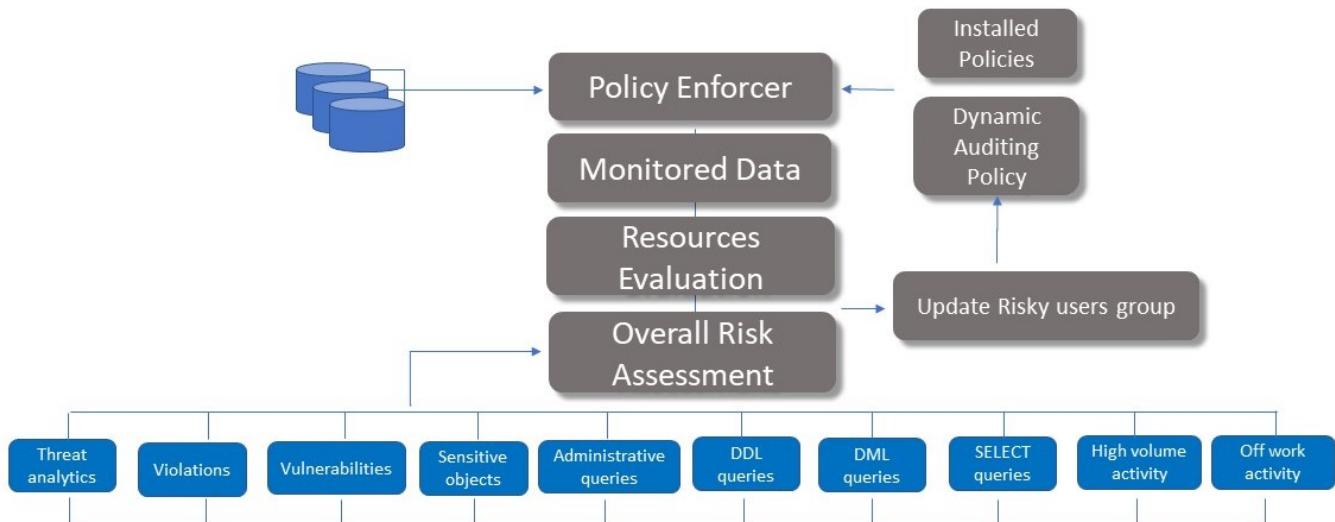
Guardium® applies the Risk Spotter algorithm to the audited data modules, to analyze multiple risk indicators and to calculate the overall risk scores of risky users.

The Risk spotter algorithm includes relevant weights of each risk indicator.

Table 1. Risk indicators used to derive total risk score per user

| Risk indicator         | Description                                                                                         |
|------------------------|-----------------------------------------------------------------------------------------------------|
| Threat Analytics       | Identified high and medium potential risks from Guardium Advanced Threat Analytics.                 |
| Violations             | The number of high and medium severity violations related to the DB user.                           |
| Vulnerability          | The number of failed vulnerability assessments for a user.                                          |
| Sensitive objects      | The number of queries on sensitive data related to the DB user.                                     |
| Administrative queries | The relative number of administrative queries related to the DB user, out of the total activity.    |
| DDL queries            | The relative amount of DDL queries related to the DB user, out of the total activity.               |
| DML queries            | The relative amount of DML queries related to the DB user, out of the total activity.               |
| Select queries         | The relative number of select queries related to the DB user, out of the total activity.            |
| High volume activity   | DB Users that have high volume activity as compared to the average of all entities of similar type. |
| Off-work activity      | Activity related to the DB user that occurred in non-work hours.                                    |

[Figure 1](#) shows how the various modules and Guardium data interact in the Risk Spotter process.



## Related concepts

- [Active Threat Analytics](#)

## Related information

- [CyberRank: Knowledge elicitation for risk assessment of database security](#)
- [Sampling high throughput data for anomaly detection for database activity](#)

## Use the Risk Spotter results

The Risk Spotter page presents risk data over your entire system, with a few graphs and tables. Learn how to use the Risk Spotter data in your daily Guardium activities.

A typical flow includes:

- View the top potential risky users.  
The Risky Users table lists the top potential riskiest users, as identified by the Risk Spotter algorithm and the Watchlist. Users from the watchlist are indicated by the eye symbol (👁) in the From Watchlist column.

With the default Latest period of time (the previous calendar day) Risk spotter shows the risk details of 50-100 users based on their activity during the previous calendar day: 50 from the Top Risky Users (highest risk score or highest potential for causing damage) and up to 50 from the Watchlist. In this scenario, the Max Risk is the same as Current Risk.

If you select Last 3 days, there are up to 150 users from the Top Risky Users group since they are aggregated over the selected time period; and up to 150 Watchlist users. In this scenario, the Max Risk column shows the highest risk for the DB user over the time period. There is one row per user. Multiple instances of both Risky User and Watchlist are aggregated into one row.

Hover over the colored risk level to see the individual risk indicators. Sort the columns to view and compare multiple occurrences of database users or databases.

- Investigate risky users in the investigation dashboard.
- If a user was added to the risky users but it seems unwarranted, add it to the Trusted users group. Henceforth, Risk Spotter only audits the user with your installed policies.
- Do you suspect other users in your system but they are not in the Risky users list? Add them to the Watchlist. Continue adding and removing users to and from the Watchlist, as relevant. View the Watchlist report, looking at maximum scores per day. Consider creating new groups and new reports for continued observation.
- Watch the Risk Spotter page, looking for trends, and unusual changes.

Auditing can be temporarily stopped for one day if system resources are low on an individual managed unit. Check the Risk Spotter log to see whether auditing was suspended.

Select one or more users from the table, and select from the Actions drop-down menu:

- View risk details: opens a window with the relative weights of the risk indicators that are currently associated with the user, for example, violations, outliers, vulnerability. The gray bars reflect the maximum score for each risk indicator based on its relative weight, and the yellow bars show the actual score. When a risk indicator reaches its maximum score, there is no gray visible. Click a risk indicator to open the [Investigation Dashboard](#), filtered for this user, database server, and verb group (if relevant), for the selected date. Click Threat Analytics in the Latest Risk or Max Risk window to open the associated Threat Analytics DB User Behavioral Analytics window.
- View max risk details: Opens a window with the relative weights of the risk indicators for the maximum identified risks that were posed by this user during the selected timeframe. Click a risk indicator to open the [Investigation Dashboard](#), filtered for this user, database server, and verb group (if relevant), for the selected date.
- Investigate: opens the [Investigation Dashboard](#), filtered for this DB user and server, for the selected date. You can investigate the specific activities that resulted in the high risk score. You can also view specific details, activities, and you can compare to other users, dates, databases. Consider adding a rule to your installed policies to quarantine the user by blocking its access on next entry.
- Assign risky user: Appears if there is no configured external ticketing system. Opens a ticket in Guardium to review specific users. (If you are logged in with the User role, add permission for the report Active Risk Spotter - Risky User before assigning a risky user.)
- Create ticket: Appears if an external ticketing system is configured. Opens a ticket in ServiceNow. See more details in [Configure an external ticketing system](#).
- Add user to Watchlist: Use the Watchlist to maintain a group of users that you want to monitor. If you try to add a user to the Watchlist, but it's currently in the Trusted Users group, the user remains in the Trusted Users group. Guardium responds with a message that at least one user was found in the Trusted Users group and was ignored. To add it to the Watchlist, you need to delete it from the trusted users group. Changes to this group are effective from the next run of the Risk Spotter.
- Add to "Risk Spotter - Trusted Users" group: Users in this group are not added to the Top Risky Users group and not monitored by the Risk Spotter policy, though they continue to be monitored by your installed policies. If you identify a false positive, consider adding the database user to the Trusted Users group. If you try to add a user to the Trusted Users group, and it's currently in the Watchlist, it's deleted from the watchlist, and added to the Trusted Users group. Changes to this group are effective from the next run of the Risk Spotter.
- Add DB users to group: Add the DB user to a group that is already defined, or create a new group. The Add DB User to Group window is prefiltered for the user. Consider adding a DB user group to a specific policy to audit these users at a higher resolution, by setting the Log Full Details option. Groups can also be used to keep watching these users with an automatic workflow process, or a specific alert. And you can use these groups in policies, and reports.
- Add server IPs to group: Add the server IP to a group that is already defined, or create a new group. The Add Server IP to Group window is prefiltered for the server IP. Consider adding a server IPs to a specific policy to audit these servers at a higher resolution, by setting the Log Full Details option. Groups can also be used to keep watching these servers with an automatic workflow process, or a specific alert. And you can use these groups in policies, and reports.

Use the Actions on risky users menu to perform:

- Audit process all risky users: This pre-defined audit process sends the Active Risk Spotter - Risky Users Scores report to the users you define. See [Building audit processes](#).
- Investigate risky users: Opens the investigation dashboard, which is filtered for the Risk Spotter - Risky Users Index group (similar to the Risk Spotter - Top Risky Users group), for the selected dates. In the Investigation Dashboard, you can look for trends over all the users. Change the time period or filters for a narrower or broader cross section, and look for patterns or other unusual behavior. Look at the distribution of activity per verb, activity over time, average activities, and errors. And drill down on specific users. See [Investigation Dashboard for data](#).
- Edit groups: where you can manage your watchlist and trusted users group – to add, remove and view members.
- View report: view one of the reports, showing data for the selected date:
  - Risky Users - Connection profiling list: the Connection profiling list report filtered for risky users
  - Risky Users - SQL Errors report: the SQL Errors report filtered for risky users
  - Risky Users - Policy Violation report: the Policy Violation report filtered for risky users
  - Active Risk Spotter - Risky Users Scores: This report lists users, DBs, total risk, and individual risk indicator scores.
  - Active Risk Spotter - Watchlist Snapshot: This report lists users, DBs, total risk, and individual risk indicator scores for the users in the Watchlist.
- Export risky users to PDF: A handy PDF, as a snapshot, or for distribution. It lists users, DBs, total risk, and individual risk indicator scores. It has the same details as the Risky Users table.
- Export risky users to CSV: A handy Excel, as a snapshot, or for distribution. It lists users, DBs, total risk, and individual risk indicator scores. It has the same details as the Risky Users table.

## Create a Dynamic Auditing policy

Learn how to create and install a policy for Dynamic Auditing, to maximize your Risk Spotter results.

### Procedure

1. Access the Policy Builder for Data.
2. Filter for Risk Assessment Dynamic Policy Selective [template], and click . The Create New Policy window opens.
3. Modify and save the policy as relevant:
  - There must be one rule with Session level criteria: Client IP/Source application/Database user/Server IP/Service name = Risk Spotter – Risky Audited Users group. This rule is included in the Risk Assessment Dynamic Policy Selective [template]. Recommended actions are Audit only or Log full details
  - Best practice: To make sure Risk spotter audits as many risky users as possible without overloading your system resources, include a rule to ignore users with high volume activity (like app users), by limiting the number of activities that are audited per user. See [limit count rule guideline](#). This rule is included in the Risk Assessment Dynamic Policy Selective [template].
  - Clear the Selective audit trail check box (in the Name and properties section) if your installed policies do not use Selective audit trail. See [Selective audit trail](#).
  - Make any other required changes.
4. Install the policy.
  - a. In the Policy Builder, select the policy and click **Install > Install**. The **Install policy** window opens.
  - b. Select an Installation action. By default the policy is installed as the last policy on the target collectors. The correct position of the risk spotter policy is based on the specific details of each installed policy. **Make sure you understand your policy details before installing the risk spotter policy.**
    - Installing the risk spotter dynamic policy first might overload system by overriding the basic session level criteria rule described in step 3.
    - Installing the risk spotter dynamic policy last might result in some risky users being ignored by prior ignore policies.

- c. Select the collectors on which to install the policy.
- d. Click OK. The system responds with a message indicating success, or not.

## Related concepts

---

- [Policies](#)

## Configure and enable Risk Spotter

Configure and enable the required and optional Guardium® and Risk Spotter modules, then enable Risk Spotter itself.

### Before you begin

---

- All collectors must be running V11.0 or later.
- Ports 8983 and 9983, on both the collectors and the central manager, are opened when you enable enterprise search. Verify that these ports are not blocked by any firewall.
- On the central manager or standalone system: Enter the GuardAPI command: **grdapic restart\_solv**.
- On the central manager: Enterprise search should be enabled by default. To check the Enterprise search status enter the following GuardAPI command:

```
grdapic get_quick_search_info
```

If it isn't enabled, enter the following GuardAPI command:

```
grdapic enable_quick_search schedule_interval=2 schedule_units=MINUTE all=true includeViolations=true
```

- Some Guardium modules must be enabled or configured before you can enable Risk Spotter. They are included in this task. You can enable the Risk Spotter process without enabling the optional Guardium modules. You get the best protection by enabling both the required and optional modules.
- Enabling Risk Spotter only activates risk assessment for users audited by your installed policies. To dynamically audit risky users with Dynamic Auditing, create and install a Risk Spotter policy. See [Create a Dynamic Auditing policy](#) and [Using the Policy Installation tool](#).

### About this task

---

Configure Risk Spotter on the central manager or on a stand-alone Guardium system. In a central manager environment, enable all modules once on the central manager only. If you install a Risk Spotter policy, this is also managed from the central manager.

Important: To maximize your Risk Spotter results, enable the optional modules.

The required modules are:

- Enterprise search: Queries data across the entire Guardium environment. It is enabled by default.
- Unit utilization data processing: Assesses resource utilization of each Guardium system in your environment to maximize user auditing. See step [3](#)
- S-TAP and buffer usage monitoring: Enables the central manager to get updated information on unit utilization and on its managed units. (Not relevant for standalone Guardium systems.) See step [4](#)

The recommended modules are:

- Dynamic Auditing: To get the most comprehensive risk assessment, configure Dynamic Auditing; create, install, and select a policy that incorporates the Risk Spotter – Audited Risky users group. This policy audits identified risky users and users in the Risk Spotter watchlist, and it samples users beyond your policy radar to identify additional risks. For details on creating the policy, see [Create a Dynamic Auditing policy](#).
- The Database Protection Subscription service (DPS) publishes updates to known vulnerabilities (known risks). The DPS file is not mandatory but without it, the risk scores are less accurate. (Best practice is to subscribe to this service whether you use Risk Spotter or not.) See step [5](#)
- Active Threat Analytics identifies various types of suspected attacks. These findings are incorporated into the Risk Spotter analysis. See step [6](#)

Click Logs and Status to open the Risk Spotter events log. This log has details of, for example: start and end of the Risk Spotter processes, if/when the risk spotter policy was uninstalled.

Note: All steps are relevant for a central manager and standalone systems unless noted otherwise.

## Procedure

---

1. Open the Risk Spotter page: go to Protect > Uncover Threat Vectors > Active Risk Spotter, and click Policy and related modules.
2. Optional: **Recommended: Dynamic Auditing**
  - a. Click Dynamic Auditing. The Configure Dynamic Auditing window opens.
  - b. Select your Dynamic Auditing policy, then click Save. The system responds: Saved. Install the policy if it's not already installed. (Only policies that use the Risk Spotter - Audited Risky Users group can be saved in this window.)
  - c. Install the policy if it's not already installed.
3. To configure Unit utilization data processing from the Active Risk Spotter UI, follow the steps in this section. Enable unit utilization to assess resource utilization of each Guardium system in your environment, and enable central manager buffer usage monitoring to assess the available bandwidth over the entire system.
  - a. Go to Manage > Unit Utilization > Unit Utilization Levels.
    - i. Configure:
      - Schedule By = Day
      - Select Days = Every Day
      - Repeat every = 1 hour
      - Each day, begin repeating at = 12:00 AM (default)
      - Select Activate Schedule
    - ii. Click Save.
    - iii. Click Run Once Now.

- b. On the central manager only (not relevant for standalone systems): Go to Reports > Report Configuration Tools > Custom Table Builder. (You must have Custom Table Builder access rights to perform this step.)
- i. In the Custom Tables page, select CM Buffer Usage Monitor and click Upload Data.
  - ii. Under Scheduling, click Modify Schedule.
    1. Leave Start time at the default 12 a.m. (midnight) ..
    2. Set Restart to every hour.
    3. Leave Repeat at Do not repeat.
    4. Set Schedule by... to Day/Week and click Every Day.
    5. Click Save.
    6. Click Back.
    7. Click Run Once Now.
  - iii. Click Back to return to the Custom Tables page.
4. To configure S-TAP information from the Active Risk Spotter UI, follow the steps in this section. On the central manager only (not relevant for standalone systems): enable S-TAP information to assess the available bandwidth over the entire system. (You must have Custom Table Builder access rights to perform this step.)
- a. Go to Reports > Report Configuration Tools > Custom Table Builder
  - b. Select S-TAP info and click Upload Data.
  - c. Under Scheduling, click Modify Schedule.
    - i. Leave Start time at the default 12 a.m. (midnight) ..
    - ii. Set Restart to every hour
    - iii. Leave Repeat at Do not repeat.
    - iv. Set Schedule by... to Day/Week and click Every Day.
    - v. Click Save.
    - vi. Click Back.
    - vii. Click Run Once Now.
5. Optional: **Recommended:** If the Database Protection Subscription service (recommended) is gray, click Upload file to open the Customer Uploads page and import a DPS file: Guardium\_V11\_Quarterly\_2019\_Q1\_20190227.enc or higher. See [Customer Uploads](#) for details on uploading and importing DPS files. (The DPS file is not mandatory, but **risk scores are partial without it.**) The DPS file can take a long time to install. If you restart the browser, the install stops. Either keep the Customer Upload window open until you see a status message, or enter the CLI command `show dps` to check install status. (DPS files are downloaded from [Fix Central](#) and [Passport Advantage](#).)
6. Optional: **Recommended:** On the central manager, enable Active Threat Analytics:
  - In the Risk Spotter page, click Configure in Active Threat Analytics Setup, expand the Active Threat Analytics processes section, and click Enable all processes. For more information, see [Active Threat Analytics setup](#).
7. Enable Risk Spotter. In the Risk Spotter page, click Enable opposite Risk Spotter process. (This button is enabled only when all required modules are enabled.)

## Results

---

It can take up to 10 minutes for the Risk Spotter page to update the number of managed units running enterprise search; or whether Active threat analytics is enabled. Go to another page, then return to this page to refresh the display.  
After the first run of the risk score process (between 01:00-02:00 daily), the Risk Spotter page shows results. The risky users are added incrementally according to the available collector resources.

## Outliers detection

Enable and start auditing outlier detection in two easy steps, letting Guardium do the work of identifying abnormal server and user behavior, and providing early detection of possible attacks.

An outlier is behavior by a particular source (in DAM either a database or a particular user on a database, and in FAM either a server or an OS user), in a particular time period or scope that is outside of the “normal” time frame or scope of the particular database or user's activity. Outliers can indicate a security violation that is taking place, even if the activities themselves do not directly violate an existing security policy.

User activity that is identified as a suspected outlier includes:

- User accessing a table for the first time
- User selecting specific data in a table that he has never selected before
- Exceptional volume of errors. For example, an application generates more SQL errors than it has in the past. This could indicate that there is a SQL injection attack in progress.
- Activity that itself is not unusual, but its volume is unusual
- Activity that itself is not unusual, but the time of activity is unusual. For example, a DBA is accessing a particular table more frequently than in the past. This could indicate that the DBA is slowly downloading small amounts of data over time.

Database activity that is identified as a suspected outlier includes:

- Exceptional volume of errors
- Activity that itself is not unusual, but its volume is unusual
- Activity that itself is not unusual, but the time of activity is unusual

Outlier Mining findings are available from the Investigation Dashboard (Quick Search) and in Reports.

Outlier mining operates on data that is already audited by a security policy. Make sure that the data you want evaluated for outliers is already audited by a security Policy.

Outlier detection can run on:

- A central manager, with data from its aggregators' collectors (except a collector that is running outliers detection locally).
- A collector, using only its own data.
- A central manager that receives data from aggregators that are managed by another CM. This is the multi-CM environment.

12.1 and later A predefined alert 'Outlier with anomaly score 90 and above', if activated, then it alerts about the outliers with anomaly score greater than or equal to 90. For more information on predefined alerts, see [Predefined alerts](#).

- [Quick start for outlier detection](#)  
Learn how to enable outliers, and start receiving alerts in a few simple steps.
- [Enabling and disabling outliers detection](#)  
Enable/disable outliers detection from any unit in a centralized environment, a multi-CM environment, or on a stand-alone collector.
- [Interpreting data outliers in the investigation dashboard](#)  
Guardium provides a convenient graphical interface for identifying and responding to outliers detected by the algorithm.
- [Interpreting file activity outliers in the investigation dashboard](#)  
View file activity monitoring outliers in the Investigation Dashboard Activity Chart and Results Table (investigation dashboard must be enabled), or review the Analytic Outlier List report.
- [Switching DB and OS users](#)  
Outlier mining, by default, tracks two types of sources: databases and database users. The behavior baseline and hourly activities are compared for each source. If your system typically has a high number of users per application, then tracking activity by DB user might not be specific enough. In this case, you can switch outliers detection user mode to evaluate by OS user. In this scenario, sources are databases and OS users. User mode is configured on the central manager for the entire system.
- [Grouping users and objects for outliers detection](#)  
Find out how to add groups, for example user or object groups, to the default outlier detection algorithm.
- [Outliers detection clustering](#)  
User clustering divides the system's users into clusters based on their activity. During the outliers scoring process, outliers detection compares the activity of the users in a group. Analyzing groups of users increases the accuracy of the results, and decreases the number of false positives.

## Quick start for outlier detection

Learn how to enable outliers, and start receiving alerts in a few simple steps.

### About this task

Outliers detection can run on any number of aggregators. However, it's recommended to start with one aggregator, refine the configuration, and then expand to additional aggregators. Before you start, decide on the available resources to investigate outliers. Then limit the number of outliers reported daily to an amount you can investigate. The Guardium algorithm provides you with the most important events to investigate, not just the "top 10," for example.

Outlier detection is a separate process from security policy rules and enforcement, so you cannot set up real-time alerts on outliers. However, because outlier data is included in reports, you can create a correlation alert. A correlation alert is triggered by a query that looks back over a specified time period to determine whether the alert threshold has been met.

### Procedure

1. Enable outliers. See [Enabling and disabling outliers detection](#), or [Active Threat Analytics setup](#).
2. Optionally fine tune the outlier definition. See [Grouping users and objects for outliers detection](#) and [Excluding events from outliers detection](#).
3. Create a query.
  - a. Navigate to Reports > Report Configuration Tools > Query-Report Builder.
  - b. Set Domain=analytic, Query name=Analytic Outliers List or Analytic Outliers Summary by Date. All other settings can be left at their defaults.
  - c. Click Create Report.
4. Create an Audit process.
  - a. Navigate to Comply > Tools and Views > Audit Process Builder.
  - b. Name the process and add the task (the report you just created).
  - c. Define receivers. Decide what kind of notifications you want. You can set up alerts, add to the to-do list, and assign users to review and justify the findings.
  - d. Schedule the process as daily, and Save.
5. For easy viewing, add the outliers reports to My Dashboard.

### Results

When the learning period is complete, there should be data in the reports, and alerts are sent.

## Enabling and disabling outliers detection

Enable/disable outliers detection from any unit in a centralized environment, a multi-CM environment, or on a stand-alone collector.

### Before you begin

- Guardium strongly recommends that you enable outliers only on 64-bit aggregators with a minimum of 24 gigabytes of memory.

### About this task

Restriction: Outliers detection and Data Level Security cannot be enabled concurrently.

Outliers detection is disabled by default. You can enable outliers detection by either of the following two ways:

- In the Maintenance > Active Threat Analytics Setup page. See [Active Threat Analytics setup](#).
- Two API commands, `enable_outliers_detection` and `disable_outliers_detection`, are used for enabling and disabling outliers detection on any Guardium system, in any topology.

The outliers detection commands affect the Guardium systems differently, depending on their setup.

#### Single CM environment

Enable outliers detection on a CM to enable/disable outliers detection on all managed units, and on all units registered to the CM thereafter, by running the API command with no additional parameters. Alternatively, you can limit the enable/disable to a list of units. Similarly, disabling outliers detection on a CM disables it on all units that are registered with the CM.

Enable outliers detection on a collector that extracts data to an aggregator. Outliers detection is enabled on the aggregator (if not already enabled) and the collector starts sending data to the aggregator. When disabling on a collector, if this is the only collector sending data to the aggregator, then the collector stops sending data, and outliers detection is disabled on the aggregator.

#### Multi-CM environment

Enable/disable outliers detection on a CM to enable/disable outliers detection on all managed units, and on all units registered to the CM thereafter, by running the API command with no additional parameters. Alternatively, you can limit the enable/disable to a list of units. Similarly, disabling outliers detection on a CM disables it on a unit registered with the CM.

When enabling on a collector that extracts data to an aggregator that is not in the same CM environment as the collector, the collector starts sending data to the aggregator, and the API responds with the name of the aggregator that needs to be enabled for outliers detection.

When enabling on an aggregator, outliers detection is enabled and collectors in the same CM environment start sending data. If the aggregator receives data from collectors in a different CM environment, the API responds with a list of all collectors that need to be enabled for outliers detection.

To enable on individual aggregators or collectors, use the commands [enable\\_outliers\\_detection\\_cross\\_cm\\_agg](#) and [enable\\_outliers\\_detection\\_cross\\_cm\\_collector](#).

#### Single Collector

Run the command on a collector that does not extract data to an aggregator to enable/disable it locally.

## Procedure

---

1. Log in to the Guardium system as a user or administrator with the CLI role.

2. To enable the outliers detection on all the units under the CM and on all units that are registered to the CM thereafter, enter: **grdapi enable\_outliers\_detection**

Optional parameters are:

- `outliers_detection_enabling`: group ID of an existing group. Relevant and optional on a CM.
- `managed_units_hostnames`: comma separated list of units. Relevant and optional on a CM.
- `FAM_DAM` is an optional parameter that specifies the type of outliers. The default is DAM.

The parameters `schedule_interval` and `schedule_units` are ignored.

3. To disable the outliers detection function, enter the command, with or without the optional parameters:

```
grdapi disable_outliers_detection
```

## Results

---

When enabling, the system starts collecting outlier data. After the learning completes(14 days), outliers data is available in the Investigation Dashboard ([Interpreting data outliers in the investigation dashboard](#) and [Interpreting file activity outliers in the investigation dashboard](#)) and the Outlier Analytic List Report.

## Related reference

---

- [Outliers detection APIs](#)

## Interpreting data outliers in the investigation dashboard

---

Guardium provides a convenient graphical interface for identifying and responding to outliers detected by the algorithm.

Quick Search must be enabled (**grdapi enable\_quick\_search**) to see outlier detection data in the investigation dashboard.

Let's say you have an outlier that shows an exceptional number of errors for user X. Some of the points you want to investigate are:

- Look at the history, is this the first time the user has outliers? The first time the user has this type of outlier?
- Comparing this user to other users, is this error type unique for this user?
- Check the error types
- Is the number of errors standard for this user?
- Look at the sensitivity of the tables accessed by the user
- Compare the actions to other DBs

Let's walk through a flow of investigating an outlier.

1. Open the investigation dashboard by selecting Data or from the User Interface drop-down, and clicking Enter; or by entering quick search in the search field and clicking Search for Data Activity, and add the Activity Chart (Add chart > Activity Chart). (You can change the time interval of the charts at the top of the window.) Red indicators reflect highly anomalous events requiring immediate attention. Yellow indicators represent less extreme anomalies that warrant attention as part of other or related investigations.

2. Hover over the outlier icon to view further details in a popup. Here you can click Show details to filter the Results Table to activities or outliers that occurred during the same time period.

3. Click the outlier to open the Summary tab of the Outlier View, which shows the number of sources that had outliers during the selected time period, and the high and medium outliers.

- Filter the data in the table either using the facets list, an individual search result, or the right-click menu.
- Use the right-click menu in the outliers table to show related activity, show related exceptions, show related violations.

4. Try monitoring only privileged users to eliminate the data and improve focus.

- You can get good insights into the patterns and usage of the privileged user activity. You might see:
  - Users that should NOT be accessing certain data.
  - SQL activity that looks abnormal, which could be privileged users that are disguising their activity with SQL attacks. See also [Characteristics of an SQL injection attack](#).

- Look for Time Of Day Outliers

5. Try monitoring only sensitive objects to eliminate the data and improve focus.

- You can get good insights into the patterns and usage of the users that access these sensitive objects. You might see unusual patterns of access to these objects.
- Look for Time Of Day Outliers.
- Look at which utilities (source programs) accessed these objects.

The Outliers tab in the Results Table has two views:

- Summary has one row per source per hour in which an outlier was found, with an anomaly score and one or more reasons. Note that not every outlier presented in the Summary Tab has further details in the Details tab.
- Details is a sample of events that occurred, with one row per event with a reason (except diverse, see table) and other details (source program, object, verb, etc.). For example, for high volume, the sampling presents the events with the highest score. You can configure the number of samples (rows) that appear in the Details Tab, per each outlier in the Summary tab.

This table describes the columns in both the Summary and Details views:

| Column name             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Further Action                                                                                                                                                                                                                                      |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Anomaly Score           | Summary Tab: A calculated aggregate value based on the volume of outliers, the severity of individual events, the predicted volume of outliers for a given time of day, and other factors. For example, on a system that typically identifies 0 outliers at 1am and 5-10 outliers at 1pm during weekdays, the presence of two additional outliers (of 2 outliers at 1am or of 12 outliers at 1pm) is more significant, and weighted more heavily, than the hourly total itself. Details Tab: The anomaly score is only relevant for a high volume event. | Right-click the score to open a menu with additional actions you can perform. In the Details tab the score can be 0, indicating that the individual events are not suspicious on their own, but the accumulated events in that hour are suspicious. |
| Textual Description     | Description of the outlier activity; may include, for example, database name, user name, object.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                     |
| High volume Outlier     | True or False. High volume of activities of some type, for example on an object, of a DB user.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                     |
| Vulnerable obj. Outlier | High volume anomaly in the activities on objects that are members of the “Temporary objects” group.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                     |
| New Outlier             | True or False. Unusual volume of object/verb activities that are not normal when compared to previous activity. For example an admin uncharacteristically creates a high number of new tables; or a user selects a number of objects and performs updates, when never performed updates earlier                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                     |
| Diverse Outlier         | Summary view only. True or False. High volume of different types of activities, for example a DB user performs many more activities than usual, or performs them at an unusual time. A sample of the diverse events does appear in the Details tab, they can be identified by the database user. Although Diverse is not a column in the details tab, they may have other reasons assigned to them. Otherwise they appear without a reason.                                                                                                              | See the Activity table for more details.                                                                                                                                                                                                            |
| Error Outlier           | True or False. High volume of errors                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                     |
| Ongoing Outlier         | Summary view only. True or False. Event in the last few hours that was not high enough to create an outlier, but does raise suspicions.                                                                                                                                                                                                                                                                                                                                                                                                                  | There are no specific events to view. See the Activity table, filter by the database in the facet list, at the time of the suspicious behavior.                                                                                                     |
| Sensitive Object        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                     |
| Number of Instances     | Details view only. Number of times this particular event has been seen in the hour.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                     |
| Records affected        | Number of records affected by the particular event. Appears as a negative number if the event does not, by definition, have affected records.                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                     |

## Related concepts

- [Anomaly Detection](#)

## Interpreting file activity outliers in the investigation dashboard

View file activity monitoring outliers in the Investigation Dashboard Activity Chart and Results Table (investigation dashboard must be enabled), or review the Analytic Outlier List report.

Quick Search must be enabled (grdapi enable\_quick\_search) to see outlier detection data in the investigation dashboard.

General workflow guidelines:

1. Open the investigation dashboard by selecting File or from the User Interface drop-down, and clicking Enter; or by entering quick search in the search field and clicking Search for File Activity, and view the outliers in the Activity Chart. (You can change the time interval of the chart at the top of the window.) Red indicators reflect highly anomalous events requiring immediate attention. Yellow indicators represent less extreme anomalies that warrant attention as part of other or related investigations.
2. Hover over an outlier icon to view detailed information about outliers detected during that time period.
3. Filter the Results Table to activities or outliers that occurred during the same time period by clicking Show details.
4. Click the outlier to open the Summary tab of the Outlier View, which shows the number of sources that had outliers during the selected time period, and the high and medium outliers.
  - Filter the data in the table either using the facets list, an individual search result, or the right-click menu.
  - Use the right-click menu in the outliers table to show related activity, show related exception, show related violations, and more.
5. Try monitoring only privileged users to eliminate the data and improve focus.
  - You can get good insights into the patterns and usage of the privileged user activity. You might see:
    - Users that should NOT be accessing certain data.
    - Look for Time Of Day Outliers
6. Try monitoring only sensitive objects to eliminate the data and improve focus.

- You can get good insights into the patterns and usage of the users that access these sensitive objects. Do this, for example, by creating a Group of file servers with sensitive data. You might see unusual patterns of access to these objects.
  - Look for Time Of Day Outliers.
  - Look at which utilities (source programs) accessed these objects.
7. Continue monitoring.
- Alerts Setting: Set alerts for the Anomaly Hours (based on Analytic Outliers Summary report)
  - Auditing: define Review Outliers (Define Audit Process on Analytic Outliers List report) and assign to the appropriate Roles / User-Groups

The Outliers tab in the Results Table has two views:

- Summary has one row per source per hour in which an outlier was found, with an anomaly score and one or more reasons. Note that not every outlier presented in the Summary Tab has further details in the Details tab.
- Details is a sample of events that occurred, with one row per event with a reason and other details. For example, for high volume, the sampling presents the events with the highest score. You can configure the number of samples (rows) that appear in the Details Tab, per each outlier in the Summary tab.

This table describes the columns in both the Summary and Details views:

| Column name         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Further Action                                                                                                                                                                                                                                      |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Anomaly Score       | Summary Tab: A calculated aggregate value based on the volume of outliers, the severity of individual events, the predicted volume of outliers for a given time of day, and other factors. For example, on a system that typically identifies 0 outliers at 1am and 5-10 outliers at 1pm during weekdays, the presence of two additional outliers (of 2 outliers at 1am or of 12 outliers at 1pm) is more significant, and weighted more heavily, than the hourly total itself. Details Tab: The anomaly score is only relevant for a high volume event. | Right-click the score to open a menu with additional actions you can perform. In the Details tab the score can be 0, indicating that the individual events are not suspicious on their own, but the accumulated events in that hour are suspicious. |
| High volume Outlier | True or False. High volume of activities of some type, for example on an object, of a DB user.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                     |
| New Outlier         | True or False. High volume of activities on new objects, for example an admin uncharacteristically creates a high number of new tables.                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                     |
| Error Outlier       | True or False. High volume of errors                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                     |
| Ongoing Outlier     | Summary view only. True or False. Event in the last few hours that was not high enough to create an outlier, but does raise suspicions.                                                                                                                                                                                                                                                                                                                                                                                                                  | There are no specific events to view. See the Activity table, filter by the database in the facet list, at the time of the suspicious behavior.                                                                                                     |
| Number of Instances | Details view only. Number of times this particular event has been seen in the hour                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                     |
| Server              | Server on which the event occurred                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                     |
| OS user             | OS User that executed the event                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                     |
| Privileged User     | True or False. Whether the user is privileged or not                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                     |
| File Full Name      | Name of file on which the user executed the event                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                     |
| Command             | Command with which the user executed the event                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                     |
| Date                | Date on which the event occurred in the format yyyy-mm-dd                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                     |
| Time                | Time at which the event occurred in the format hh:mm:ss                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                     |

## Related concepts

- [Investigation Dashboard](#)
- [Anomaly Detection](#)

## Related reference

- [Outliers detection APIs](#)

## Switching DB and OS users

Outlier mining, by default, tracks two types of sources: databases and database users. The behavior baseline and hourly activities are compared for each source. If your system typically has a high number of users per application, then tracking activity by DB user might not be specific enough. In this case, you can switch outliers detection user mode to evaluate by OS user. In this scenario, sources are databases and OS users. User mode is configured on the central manager for the entire system.

## About this task

All managed units that report to one central manager use the same mode.

You usually switch user mode only once on your system, preferably before you enable outliers detection. When you switch user mode, all the statistical modeling on the DB users is discarded, and the system starts over again, collecting details on the OS user.

In a cross-CM environment, you need to switch the mode on both central managers (or all central managers that share a collector-aggregator link).

If you have managed units that are running a version earlier than V11.2, they continue to accumulate data for DB users. They are identified in the Active Threat Analytics Setup page by the text User Mode change requires V11.2+.

If you are already running outliers detection, and specific events are excluded from the outliers detection algorithm (the Ignore option in the investigation dashboard), then:

- The value of each ignored field is maintained when you switch between DB and OS user.
- The ignored field is now the OS user and not the DB user.

You must evaluate each Ignore statement and decide whether you want to keep it or not. Since DB users and OS users rarely, if ever, have the same names, excluded events are usually deleted, and new ones defined. In the Analytic User Feedback, rows that have a value for DB user now show a value for OS user.

## Procedure

---

1. Evaluate each Ignore statement and decide whether it's relevant for an OS user.
  - a. Open the Analytic User Feedback report to view ignored events.
  - b. To delete an ignored event, double-click the event, and select Invoke > delete\_analytic\_user\_feedback.
2. On the central manager, switch to OS users by running the API command **set\_outliers\_user\_detection\_mode mode=OS**  
This command disables outlier mining on all units in the system, switches the user mode, and enables outlier mining on all units that were running outliers mining before the switch. The mode is listed in the Active Threat Analytics Setup page.
3. If a managed unit was unavailable when you switched users, as seen in the Active Threat Analytics Setup page, disable outlier mining on that unit, and then enable outlier mining. The mode switches.

## Grouping users and objects for outliers detection

---

Find out how to add groups, for example user or object groups, to the default outlier detection algorithm.

## About this task

---

By default, there are two groups of users and objects that are weighted or scored more heavily by Guardium® machine-learning algorithm: Admin Users and Sensitive Objects. However, you may have already established additional groups that would also be useful for outlier detection. For example, you may have a group of Suspicious Users or you may have several different groups of sensitive objects that are aligned with different applications.

## Procedure

---

1. This task requires that you know the internal group ID to use with the grdapi command. To get the group ID, you can use the following command: `grdapi list_group_by_desc desc=[group name]`. For example, if you have a group named BadGuys, you can enter the following command to get its internal group ID:  
`grdapi list_group_by_desc desc="BadGuys"`
2. Once you know the desired ID, add it as privileged user group for a boosted score as follows (note that you must also include the default group 1 if you want to boost scores for that as well). To add a group with the ID 1234: `grdapi set_outliers_detection_parameter parameter_name="privUsersGroupIds" parameter_value=1,1234`
3. To add sensitive objects with the IDs 333 and 156: `set_outliers_detection_parameter parameter_name="sensitiveObjectGroupIds" parameter_value=5,333,156`

## Results

---

The specified groups or sensitive objects are added to the outlier detection and are given additional weight by the algorithm.

## Outliers detection clustering

---

User clustering divides the system's users into clusters based on their activity. During the outliers scoring process, outliers detection compares the activity of the users in a group. Analyzing groups of users increases the accuracy of the results, and decreases the number of false positives.

When a user's activity is unusually high, or has many errors, Guardium compares its activity with its cluster's activity and changes the user scores, as relevant.

The clustering algorithm runs periodically, moving users into a different cluster group as relevant. The outlier log /opt/IBM/Guardium/analytic/outlier\_out/outlier.log details changes in the outliers scoring process. (The userClustering.log, also in this folder, is used by support only.)

User clustering is enabled by default. It's recommended to leave the configuration at its default. The configuration is controlled with the API command `set_outliers_detection_parameter` parameters.

- `clusteringScheduleIntervals`: The frequency, in hours, at which the clustering algorithm runs.
- `minNumIntervalsForFirstClustering`: the number of periods, in hours, until the initial clustering of users.

To disable the user clustering, set both of these parameters = 0.

## Related reference

---

- [set\\_outliers\\_detection\\_parameter](#)

## Real-time trust evaluator

---

The Real-time Trust Evaluator (RTTE) evaluates the application connections that are monitored by Guardium®. Connections are classified as "untrusted", "evaluated" or "trusted". Trust scores (value from 0 - 100) are assigned to each classified connection. Connections that are not classified as trusted or untrusted are classified as evaluated.

The trust evaluator release consists of the following main modules:

1. Security incident policies that are capable of detecting denial-of-service attacks, credential stuffing attacks, password-spraying attacks, and connection authentication vulnerabilities.  
Note: You cannot modify the trust evaluator policies.
2. Probabilistic engine (Probability engine), based on a Bayesian machine learning model. This model requires a long training period. The training status is displayed in the user interface so that you can follow it.
3. Anomaly detection, based on a special machine learning model. Visually, anomaly detection is represented as a list of anomaly conditions. This model requires a short training period and training status is not displayed.

All three modules evaluate application connections in parallel.

The evaluated application connections are collected. The trust evaluator is integrated with session level policies. Thus, a session level policy installed outside the trust evaluator can be used to alert customers of security breaches, create security exceptions, and terminate connections if necessary. For more information, see [Session-level policies](#).

Note: The trust evaluator is available from central manager and standalone machines only. In addition, all collectors must be at Guardium 11.4 or later. When using the trust evaluator, it's best to manage policies from the central manager. This avoids situations where enabling the trust evaluator causes the central manager to overwrite policies that may have been updated on managed units but not yet synced to the central manager. If you must manage policies from managed units, wait until any policy changes are synced to the central manager before enabling the trust evaluator.

## Getting started

---

To get started with the real-time trust evaluator, browse to Protect > Security Policies > Real-Time Trust Evaluator from a central manager and click Enable.

When the trust evaluator starts up, it installs security incidents policies, and begins to evaluate incoming connections. At the same time, the probability engine enters its first training phase.

Here's what you need to know:

- You can view the evaluated application connections from the connections window. For more information, see [Configuring the connections table](#).
- When you click Enable, the trust evaluator installs the security incident policies. You can use the default, **Real-time trust evaluator: incidents related to all users**, or select a different policy from the Configuration section. For more information, see [Configuring the trust evaluator](#).
- When you click Disable, the trust evaluator stops and uninstalls the security incidents policy.
- For anomaly detection, you can select anomalies from the [Anomalies tab](#).

The remainder of this topic provides more information about how the trust evaluator works, configuration information, and details about the connection table and information graphs.

## How the trust evaluator works

---

When you first start the trust evaluator, it begins to evaluate application connections by using installed security incident policies. At the same time, probability engine and anomaly detection modules start their training phases.

At this point, trust evaluator can detect untrusted application connections. Untrusted application connections include security violating connections such as communicating with plain passwords, performing denial-of-service credential stuffing or password-spraying attacks, administrative communicating with not encrypted information, and so on. The trust evaluator sets low trust scores to detected untrusted connections.

When the probability engine finishes its training, it starts to evaluate application connections as well. Connections can be evaluated as "untrusted", "evaluated" or "trusted".

When the anomaly detection module finishes its training, it also starts to evaluate application connections. Connections can be evaluated as "evaluated".

## Trusted versus untrusted connections

---

The trust evaluator identifies a connection as trusted when it meets one of the following criteria:

- The connection matches the criteria of the trusted connection group.
- The probability engine deems that the connection is sufficiently common.

A connection is identified as untrusted in the following circumstances:

- A connection that is identified by a security incident policy as a threat.
- A user-supplied untrusted group.
- In addition, there can be multiple factors and parameters that identify the trustworthiness of a connection. The probability engine can assign an untrusted score if it is not similar to known data, or if other trust evaluator components identify issues for that connection. For example, you might have a case where the probability engine identifies a connection as trusted, but an anomaly or incident is identified for the connection. In this case, the connection is identified as untrusted.
- [Configuring the trust evaluator](#)  
When you configure the trust evaluator, you can choose to monitor either all connections (the default) or administrator connections.
- [Viewing trust evaluator status](#)  
The Status window shows the progress of the probability engine as it learns the typical behaviors of traffic for your system.
- [Adding post-training automation](#)  
After your system is trained and running, the trust evaluator continues to monitor all of your connections, and displays them in the connections table.
- [Configuring the connections table](#)  
From the connections table, you can manage and view information about your connections.

## Configuring the trust evaluator

---

When you configure the trust evaluator, you can choose to monitor either all connections (the default) or administrator connections.

From the Configuration section of the Real-Time Trust Evaluator window, you can see the current settings for the trust evaluator. The default settings are shown on the trust evaluator page. Each setting is associated with one of the configuration tabs.

- Learn patterns from scratch.
- Run on all collectors.
- Evaluate all sessions for all users.
- Use default trust thresholds.
- Evaluate 12 of 12 anomalies.

To change the default settings, click Configure to open the Configure trust evaluator window. From here, you can use the following tabs to configure your system. However, you can also choose to use the defaults and click Enable to install the **Real-time trust evaluator: incidents related to all users** policy and start the training.

When you are done configuring the trust evaluator, click Save to save your changes. At this point, you can click Enable from the trust evaluator main page to begin training your system.

## Inputs tab

From Inputs, you can specify groups of explicitly trusted or untrusted connections. When you add an existing group, the trust evaluator adds those connections to the specified list.

- If you select a group from the Trusted connections list (for example, Risk Spotter - Trusted Users) the trust evaluator continues to monitor the connections. If a connection encounters a security incident, it is removed from the trusted connections and added to untrusted connections.
- If you select a group from the Untrusted connections list (for example, Risk Spotter - Top Risky Users) the trust evaluator assumes that the connections are never trusted. The trust evaluator does not include the connections that are specified as untrusted in the training.

Select Do not consider client IP as part of connection analytics to ignore client IP addresses during trust-score evaluation. This option is useful when the client IP address changes frequently, for example if your site uses dynamic or virtual IP addresses.

## Systems tab

From Systems, you can make the following changes:

- Select the collectors that you want to include in the trust evaluator. The trust evaluator runs only on a central manager, the Systems page displays the related collectors. You can select one of the following system groups:
  - All Collectors: Display all of the collectors associated with this central manager.
  - All Units group: Display all available machines associated with this central manager.
- Alternatively, also use the filter box to find and display specific machines by name or number.
- After you select the machines that you want to include in the trust evaluator training, you can take one of the following steps:
  - Click Collectors to include all of the selected machines.
  - Select each machine that you want to include.

## Incidents tab

From Incidents, you can choose incidents that are related to all users or only incidents that are related to administrators.

For each type of incident (administrator or all users), Guardium® surfaces a read-only policy that you can view from the Security Policies page (Policies > Security Policies > Policy Builder for Data). Depending on your selection, the trust evaluator uses one of the following session-level security incident policies.

Each policy provides a number of rules that track and report on possible security incidents that might be encountered at run time:

- **Real-time trust evaluator: incidents related to all users**
- **Real-time trust evaluator: incidents related to administrative users**

The rules for each policy are described under [Security incident policies](#).

- For information about incidents related to all users, see [All users](#).
- For information about incidents related to administrative users, see [Administrative users and applications](#).

When you enable the trust evaluator, Guardium installs the selected policy before training.

From Incidents, you can select and modify groups against which to run the trust evaluator. If you do not select any groups here, the trust evaluator runs against all server IP addresses associated with the selected S-TAP.

Note: If you select Incidents related to administrators, make sure that the groups you select include only populated groups. If you select an empty group, there are no members of the group to test against. Therefore, the trust evaluator cannot find security incidents for the empty group, but does not provide any indication that the group is not populated.

## Thresholds tab

From Thresholds, you can view or change the trust-score thresholds that the trust evaluator uses to mark connections as trusted, untrusted, or evaluated (that is, not trusted or untrusted). As you start to understand your system, you can tweak the default trust scores (90 or greater for trusted, 10 or lower for untrusted) to help ensure that your system is protected.

## Anomalies tab

When training begins, the anomalies engine tracks unique connections. The trust evaluator starts to recognize anomalies after it sees a sufficient number of unique connections. When any anomalies are found, they are logged in the **Connection Exceptions** report.

Note: The number of "sufficient connections" to detect anomalies is based on your environment and set without user involvement, but it is always greater than 1000 connections.

From Anomalies, select some or all of the anomaly conditions. The trust evaluator uses the read-only Real-time trust evaluator: Security anomalies policy, where each rule represents an anomaly type. For more information about the Security anomaly policy, see [Security anomalies](#).

## Related concepts

- [Session-level policies](#)

## Related reference

- [Security incident policies](#)

## Viewing trust evaluator status

The Status window shows the progress of the probability engine as it learns the typical behaviors of traffic for your system.

Click View status to open the Status window.

Note: The status includes PAUSED or IDLE when no traffic is seen for at least 15 minutes. When Guardium detects traffic again, the trust evaluator restarts, the status updates.

Table 1. Status types

| Status                | Meaning                                                                                                                                                                                                                                                               |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FIRST STAGE LEARNING  | The initial 7-day learning period.                                                                                                                                                                                                                                    |
| SECOND STAGE LEARNING | The secondary 24-hour contiguous learning period                                                                                                                                                                                                                      |
| TRAINED               | Training is complete. Guardium is issuing trust scores.                                                                                                                                                                                                               |
| RETRAINING            | Issuing trust scores using current learning data. However, Guardium is training a secondary model in the background. When learning completes the old model is quietly replaced.                                                                                       |
| IMMEDIATE RETRAINING  | Guardium discards the current training data and begins the training from the first stage. This status generally indicates that Guardium found too many anomalous connections. The probability engine will discard the current training data and retrain from scratch. |

## Adding post-training automation

After your system is trained and running, the trust evaluator continues to monitor all of your connections, and displays them in the connections table.

For a trained system, you can determine the actions to take when connections are marked as trusted, untrusted, or evaluated (but not categorized as trusted or untrusted).

- Select Automation, and then, for each category type, select an appropriate action and an optional group.  
If you specify an existing group, or add a new group, the identified connections (trusted or untrusted) are automatically added to that group.  
For more information about the available actions, see [Policy rule actions](#).
- When you are done, click Save to save your changes and close the Automation window.

Deciding when to use automation depends on how your site is configured. However, some guidelines for automation are as follows:

- Before you enable automation, review all of your connections to ensure that both trusted and untrusted connections align with your expectations.
- Guardium suggests that you ignore trusted connections only for trusted group input connections or for trusted connections that you review regularly.
- If you set untrusted connections to one of the S-GATE Session *Terminate* actions, be aware that your users may notice if some connections are terminated.

## Configuring the connections table

From the connections table, you can manage and view information about your connections.

While the trust evaluator runs (either during or after training), you can use Time frame to set the number of days of connections to display in the connections table.

From the connections table, you can take the following steps:

- Select the type of connections you want to view (Trusted, Evaluated (but not categorized as trusted or untrusted), or Untrusted).  
Note: If the real-time trust evaluator encounters multiple incidents for the same connection (for example, an administrator who uses the same password for multiple accounts), then only the first incident might be recorded in the connections table.
- Use the Filter box within connection types to create a subset of connections.
- Click  to download information about all of the connections that are shown in the connections table.
- Select one or more connections from the table and then select Actions. You can add the selected connections to the Trusted connections group, the untrusted connections group, or to a custom group.  
If you select Add to custom group, the Add to custom group window displays. The group type must be *Tuples*, but you can either select an existing group or create a new group. For more information about tuple groups, see [Groups overview](#).

After you save and close the custom group, the selected connections are added to the group.

- Select Hide connections in trusted groups (or Hide connections in untrusted groups) to hide any connections that match existing members in a trusted or untrusted group. When you select this option, only the trusted (or untrusted) connections found by the trust evaluator display in the connections table. The results reason

shows as **Trusted as input from user** or **Untrusted as input from user**.

In addition, two graphs display the data from the connections table.

- The Connections seen or evaluated graph displays the total number of connections that have been seen or evaluated by the trust evaluator. The graph includes connections that are known to be untrusted (and therefore not evaluated), as well as connections that are not yet evaluated (new connections). The number in the center of the graph reflects one of the following numbers:
  - If your mouse is not in the graph, the number reflects the total number of connections that were seen or evaluated in the selected timeframe.
  - If you hover your mouse over one of the graph elements, the number reflects the number of connections that are represented by the graph element (that is: new, trusted, evaluated, or untrusted).
- The Trust scores assigned graph shows the number of connections in each trust score category and the percentage of connections in each category. Categories are labeled as 0 - 10, 11 - 20, and so on). This graph does not include new connections that are not yet evaluated.

## Policies

Policies are sets of rules and actions applied in real time to the database traffic observed by a Guardium system. Policies define which traffic is ignored or logged, which activities require more granular logging, and which activities should trigger an alert or block access to the database.

- **[Understanding policies](#)**  
A security policy contains an ordered set of rules to be applied to the observed traffic between database clients and servers. Each rule can apply to a request from a client, or to a response from a server. Multiple policies can be defined and multiple policies can be installed on a Guardium appliance at the same time.
- **[Session-level policies](#)**  
Session-level policies and advanced session-level policies create new possibilities for detecting suspicious behavior of users of services as well as security incidents. Session-level policies are created using the Policy Builder for Data, and advanced session level policies are created as scripts using the SR language and uploaded to Guardium using the Policy Builder for Data.
- **[Policy rule actions](#)**  
Define blocking, alerting, or logging actions to take when policy rules are matched.
- **[Creating and installing a policy and policy rules](#)**  
Use the Policy Builder for Data to manage policies and policy rules.
- **[Tagging policy rules](#)**  
Guardium provides predefined policy rule tags and supports custom tagging of rules. Use tags to quickly create and manage policies aligned with specific compliance standards, reporting and auditing requirements, or geographies.
- **[Using the Policy Installation tool](#)**  
Learn how to install a policy on your Guardium system.
- **[Running policy analyzer and reviewing results](#)**  
Policy analyzer provides insights that help identify frequently fired rules, optimize rule order, and evaluate rule changes.
- **[Security incident policies](#)**  
Guardium® provides several session level policy templates that encapsulate security problems that are frequently found at run time.

## Understanding policies

A security policy contains an ordered set of rules to be applied to the observed traffic between database clients and servers. Each rule can apply to a request from a client, or to a response from a server. Multiple policies can be defined and multiple policies can be installed on a Guardium appliance at the same time.

Each rule in a policy defines a conditional action or several actions. The condition tested can be a simple test - for example it might check for any access from a client IP address that does not belong to an Authorized Client IPs group. Or the condition tested can be a complex test that considers multiple message and session attributes (database user, source program, command type, time of day, etc.), and it can be sensitive to the number of times the condition is met within a specified time frame.

The action triggered by the rule can be a notification action (e-mail to one or more recipients, for example), a blocking action (the client session might be disconnected), or the event might simply be logged as a policy violation.

A policy violation is logged each time that an alert or log-only action is triggered. Optionally, the SQL that triggered the rule (including data values) can be recorded with the policy violation. Policy violations can be assigned to incidents, either automatically by a process, or manually by authorized users (for more information, see [Incident Management](#)).

Attention: Correlation alerts can also be written to the policy violations domain (for more information, see [Managing correlation alerts](#)).

In addition to logging violations, policy rules can affect the logging of client traffic, which is logged as constructs and construct instances.

- Constructs are prototypes of requests that Guardium® detects in the traffic. The combinations of commands, objects and fields included in a construct can be very complex, but each construct represents a specific type of access request. The detection and logging of new constructs begins when the inspection engine starts, and by default continues (except as described) regardless of any security policy rules.
- Each instance of a construct detected in the traffic is also logged, and each instance is related to a specific client-server session. No SQL is stored for a construct instance, except when a policy rule requests the logging of SQL for that instance, or for a particular client/server session of instances (with or without values).

In addition to controlling the inclusion of SQL in client construct instances, a security policy rule can disable the logging of constructs and instances for the remainder of a session.

In heavy volume situations, the parsing and aggregating of information into constructs and instances can be deferred by using the Log Flat (Flat Log) option. When used, the production of alerts and reports will be delayed until the logged information has been aggregated.

To completely control the client traffic that is logged, a policy can be defined as a selective audit trail policy. In that type of policy, audit-only rules and an optional pattern identify all of the client traffic to be logged.

Data-monitoring policies are installed from Protect > Security Policies > Policy Builder for Data or from Protect > Security Policies > Policy Installation.

Attention: On a new installation only (not on upgrades), a default policy is installed. It contains one rule, and the policy name is Default - Ignore Data Activity for Unknown Connections.

- **[Rule types, categories, classifications](#)**  
Within a policy, rules are evaluated in the order in which they appear as each element of traffic is analyzed.
- **[Minimum counts and reset intervals](#)**  
Some activities are normal and acceptable when they occur less than a certain rate but require attention when the rate exceeds a tolerable threshold.
- **[Continue to next rule](#)**  
By default, the evaluation of access and exception rules for a unit of traffic ends when a rule is triggered provided there are not multiple actions in one rule. In cases where it is necessary to take multiple actions for the same or similar conditions, enable the Continue to next rule setting for that rule.
- **[Record values with policy violation](#)**  
When using the Record values setting, the actual construct causing the rule to be satisfied will be logged in the SQL string attribute and is available in reports.
- **[Values and groups of values in rules](#)**  
For many policy rule criteria, you can specify a single value or a group of values. It is also possible to simultaneously specify both a single value and a group of values.
- **[Matching patterns with regular expressions](#)**  
Use regular expressions to search traffic for complex data patterns.
- **[Special pattern tests](#)**  
You can use these special pattern tests to identify sensitive data that is contained in the traffic that flows between the database server and the client.
- **[Log flat](#)**  
Log flat allows Guardium to log information without immediately parsing it.
- **[Rules on flat](#)**  
The rules on flat setting changes the way Guardium processes policy rules.
- **[Selective audit trail](#)**  
When you create or edit a policy, click Selective audit trail to limit the amount of logging on the Guardium system.
- **[Analyzer rules](#)**  
Certain rules can be applied at the analyzer level.
- **[Character sets](#)**  
You can use character set codes in extrusion rules.

---

## Rule types, categories, classifications

Within a policy, rules are evaluated in the order in which they appear as each element of traffic is analyzed.

There are three types of rules:

- An access rule applies to client requests. For example, it might test for UPDATE commands issued from a specific group of IP addresses.
- An exception rule evaluates exceptions returned by the server (responses). For example, it might test for five login failures within one minute.
- An extrusion rule evaluates data returned by the server (in response to requests). For example, it might test the returned data for numeric patterns that could be social security or credit card numbers.

For each rule, an optional Category and Classification can be assigned. These are used to group policy violations for both reporting and incident management.

---

## Minimum counts and reset intervals

Some activities are normal and acceptable when they occur less than a certain rate but require attention when the rate exceeds a tolerable threshold.

For example, if interactive database access is allowed, a consistent but relatively low rate of login failures might be expected. However, a sharply higher rate might indicate an attack is in progress.

To deal with thresholds, a minimum count and a reset interval can be specified for each policy rule. For example, this can be used to trigger the rule action after the count of login failures exceeds 100 (the minimum count) within one minute (the reset interval). If omitted, the default is to execute the rule action each time the rule is satisfied.

---

## Continue to next rule

By default, the evaluation of access and exception rules for a unit of traffic ends when a rule is triggered provided there are not multiple actions in one rule. In cases where it is necessary to take multiple actions for the same or similar conditions, enable the Continue to next rule setting for that rule.

The Continue to next rule setting applies to access rules following access rules and to exception rules following exception rules. It does not apply to an exception rule following an access rule or an access rule following an exception rule.

Extrusion rules will be processed regardless of the end of an access or exception rule preceding the extrusion rule.

In the session level policies, Continue to next rule setting applies to the rules that have alerting and logging actions.

---

## Record values with policy violation

When using the Record values setting, the actual construct causing the rule to be satisfied will be logged in the SQL string attribute and is available in reports.

When the Record values setting is not used, no SQL statement is logged.

To include the full values in the policy violation, set the Record values parameter to 1 - Log full SQL in policy violation for that rule.

Attention: The full SQL with values will be available only in the policy violation record within the policy violations reporting domain. It will not be available in the client traffic log or on reports from the data access domain. To include full SQL (with or without data values) in the client traffic log, use the Log Full SQL rule action.

## Values and groups of values in rules

For many policy rule criteria, you can specify a single value or a group of values. It is also possible to simultaneously specify both a single value and a group of values.

Be aware that a group member may contain wildcard (%) characters, so each member of a group may match multiple actual values.

- Negative rules: use the != or Not in group operators to create a negative rule. For example, not the specified Application user or not any member of the selected group. It is also possible to exclude both single values and a group of values. For example, define two negative Application user rule criteria, one using != for a specific user and another using Not in group to exclude members of a selected group.
- Empty value: enter the special value `guardium://empty` to test for an empty value in the traffic. This is allowed only in the following fields: Application event text, Application user, Database name, Database user, Event type, Event user name, Operating system user, and Source application.
- Define a new group to be tested: select the In group or Not in group operator and click the  icon to define a new group.
- Match any value: select the = operator and leave the value field blank.
- Match a specific value: select the = operator and enter the value to match in the text field.
- Match any member of a group: select the In group operator, select the group from the list of groups. If the minimum count is greater than one, there will be a single counter, and it will be incremented each time any member of the group is matched.
- Match an individual value or any member of a group: define two rule criteria, one using the = operator to match a specific value and another using In group to match members of a selected group. If the minimum count is greater than one, there will be a single counter, and it will be incremented each time the individual value or any member of the group is matched.
- If the minimum count is greater than one, count each individual value separately: select the = operator and enter a period (.) in the value field. Note that the period option cannot be used for the Service name or Network protocol criteria.
- If the minimum count is greater than one, count each member of a group separately: select the In group operator and select a group from the list.

## Matching patterns with regular expressions

Use regular expressions to search traffic for complex data patterns.

The Guardium implementation of regular expressions conforms with PCRE, which differs from the UNIX implementation of regular expressions. Regular expressions are allowed in any field that is followed by the  button.

Restriction: Guardium does not support regular expressions for non-Latin character sets.

However, if your database uses UTF-8 encoding for Unicode, you can use the |xnn pattern to extend regex patterns in Unicode data, to, for example, scrub data written in non-Latin character sets. Technically, you can now scrub any data that you can represent with |xnn byte patterns. However, there are some limitations, as follows:

- Each database has its own encoding scheme. You need to know which Unicode encoding your database uses.
- The replacement character in scrub might not appear the same as defined in the scrub pattern, especially with 2-byte encoding schemes.
- To limit the scrub, specify the length of the data to scrub as prefix. Otherwise, you might override the query metadata, which can lead to a failure or crash.

Tip: You can also use regular expressions with the following criteria by typing the special value `guardium://regexp/(regular expression)` in the value field: Database user, Application user, Source application, Field name, Object, Application event values text.

Notes:

- If a complex regex statement fails (for example, a statement that uses recursive stack matching up to the maximum depth of the stack), criteria matching stops and the error is logged to the snif log. However, one error is logged at most every 30 minutes (and not for each failed statement).
- Redact policies that use regular expressions can only scrub null-terminated data types.

For more information about using regular expressions, see [Regular Expressions](#). For more information about troubleshooting with REDACT and regex, see [REDACT function causes overly masked result](#) and [REDACT - Working with regex on Windows DB servers](#).

## Special pattern tests

You can use these special pattern tests to identify sensitive data that is contained in the traffic that flows between the database server and the client.

Each policy rule can include a single special pattern test. To use one of these tests, begin the rule name with one of the special pattern test names, followed by a space and one or more additional characters to make the rule name unique. For example, if you are searching for Social Security numbers of your employees, you could name the rule `guardium://SSEC_NUMBER_employee`. You can still specify all other components of the rule, such as specific client and server IP addresses.

These tests match a character pattern, and that match does not guarantee that the suspected item, such as a Social Security number, has been encountered. There can be false positives under a variety of circumstances, especially if longer sequences of numeric values are concatenated in the data.

`guardium://CREDIT_CARD`

Detects credit card number patterns. It tests for a string of 16 digits or for four sets of four digits, with each set separated by a blank. This special pattern test also works with American Express 15-digit credit card number patterns (first digit 3 and second digit either 4 or 7). For example: **1111222233334444** or **1111 2222 3333 4444**

When a rule name begins with "guardium://CREDIT\_CARD", and there is a valid credit card number pattern in the Data pattern field, the policy uses the Luhn algorithm, a widely-used algorithm for validating identification numbers such as credit card numbers, in addition to standard pattern matching. The Luhn algorithm is an additional check and does not replace the pattern check. A valid credit card number is a string of 16 digits or four sets of four digits, with each set separated by a blank. There is a requirement to have both the `guardium://CREDIT_CARD` rule name and a valid [0-9]{16} number in the Search Expression box in order to have the Luhn algorithm involved in this pattern matching.

`guardium://PCI_TRACK_DATA`

Detects two patterns of magnetic stripe data. The first pattern consists of a semi-colon (;), 16 digits, an equal sign (=), 20 digits, and a question mark (?), such as:

**;1111222233334444=11112222333344445555?**

The second pattern consists of a percent sign (%), the character B, 16 digits, a carat (^), a variable-length character string terminated by a forward slash (/), a second variable-length character string terminated by a carat (^), 31 digits, and a question mark (?), such as:

**%B1111222233334444^xxx/xxxx x^1111222233334444555566667777888?**

guardium://SSEC\_NUMBER

Detects numbers in Social Security number format: three digits, dash (-), two digits, dash (-), four digits, such as **123-45-6789**. The dashes are required.

guardium://CPF

The Cadastro de Pessoas Físicas (CPF), a Brazilian personal identifier. It contains 11 digits of the format **nnn.nnn.nnn-nn**, where the last two digits are check digits. Check digits are computed from the original nine digits to provide verification that the number is valid. The formatting characters within the expression are optional. If there is a match on the expression, the check digits are validated.

guardium://CNPJ

Cadastro Nacional de Pessoas Jurídicas (CNPJ), an identification number used for Brazilian companies. It contains 14 digits of the format **00.000.000/0001-00** where:

- The first eight numbers show the registration.
- The next four numbers identify the entity branch. 0001 is the default value for head quarters.
- The last 2 numbers are the check digits.

The formatting characters within the expression are optional. If there is a match on the expression, the check digits are validated.

12.1 and later

guardium://CANSIN

Detects Canadian Social Insurance Number (SIN) pattern.

When a rule name begins with 'guardium://CANSIN', and there is a valid SIN number pattern in the data pattern field, the policy uses the Luhn algorithm, a widely-used algorithm for validating identification numbers such as credit card numbers, in addition to standard pattern matching.

## Log flat

Log flat allows Guardium to log information without immediately parsing it.

This saves processing resources, so that a heavier traffic volume can be handled. The parsing and merging of that data to Guardium's internal database can be done later, either on a collector or an aggregator unit.

There are two Guardium features involving the Flat Log Process - Flat Log by policy definition and Flat Log by throttling mechanism.

Flat Log by throttling mechanism - This is the feature implemented by running the CLI command, store alp\_throttle 1. The same policy that is applicable to real-time S-TAP traffic is used to process traffic that was logged into the GDM\_FLAT\_LOG table.

For Flat Log by throttling mechanism, the Flat Log checkbox should NOT be checked in Policy Builder.

Flat Log by policy definition - Selection of this feature involves the Policy Builder menu in Setup >Tools and Views and Flat Log Process menu in Manage > Activity Monitoring.

Note: Rules on flat does not work with policy rules involving a field, an object, SQL verb (command), Object/Command Group, and Object/Field Group. In the Flat Log process, "flat" means that a syntax tree is not built. If there is no syntax tree, then the fields, objects and SQL verbs cannot be determined.

The following actions do not work with rules on flat policies: LOG FULL DETAILS; LOG FULL DETAILS PER SESSION; LOG FULL DETAILS VALUES; LOG FULL DETAILS VALUES PER SESSION; LOG MASKED DETAILS.

When the Log Flat (Flat Log) checkbox option listed in the Policy Definition screen of the Policy Builder is checked,

- Data will not be parsed in real time .
- The flat logs can be seen on a designated Flat Log List report.

## Rules on flat

The rules on flat setting changes the way Guardium processes policy rules.

When Rules on flat is checked:

- Session-Level rules will be examined in real-time.
- No rules will be evaluated when the offline processing does takes place.

When Rules on flat is NOT checked:

- Policy rules will fire at processing time using the current installed policy.

Note: Rules on flat does not work with policy rules involving a field, an object, SQL verb (command), Object/Command Group, and Object/Field Group. In the Flat Log process, "flat" means that a syntax tree is not built. If there is no syntax tree, then the fields, objects and SQL verbs cannot be determined.

The following actions do not work with rules on flat policies: LOG\_FULL\_DETAILS; LOG\_FULL\_DETAILS\_PER\_SESSION; LOG\_FULL\_DETAILS\_VALUES; LOG\_FULL\_DETAILS\_VALUES\_PER\_SESSION; LOG\_MASKED\_DETAILS.

## Selective audit trail

When you create or edit a policy, click Selective audit trail to limit the amount of logging on the Guardium system.

A selective audit trail is appropriate in the following circumstances.

- The traffic of interest is a relatively small percentage of the traffic that the inspection engines.
- All of the traffic you might ever want to report upon can be completely identified.

For any Guardium collector, if Selective audit trail is specified for one policy, then all policies for that collector use a selective audit trail. In this case, multiple policies are treated as a single policy, where rules are applied in the order that the policies are installed.

Without a selective audit trail policy, the Guardium appliance logs all traffic that the inspection engines accept. Each inspection engine on the appliance or on an S-TAP is configured to monitor a specific database protocol (Oracle, for example) on one or more ports. In addition, the inspection engine can be configured to accept traffic from subsets of client/server connections, which tends to capture more information than a selective audit trail policy. However, it might cause the Guardium appliance to process and store more information than is needed to satisfy your security and regulatory requirements.

When a selective audit trail policy is installed, only the traffic that the policy requests is logged. Traffic is identified in two ways:

- Specify a string to use to identify the traffic of interest in the Audit Pattern box of the Policy Definition window. You might identify a database or a group of database tables, for example. An audit pattern is a pattern that is applied (via regular expression matching) to EACH SQL that the logger processes to see whether it matches. This pattern match is strictly a string match. It does not match against the session variables (such as DB name) the way the policy rules do.
  - Specify Audit Only or any of the Log actions (except for Log Full Details Per Session) for one or more policy rules in a Rule Definition window. With policy rules you can be precise, specifying exact values, groups, or patterns to match for every conceivable type of attribute (such as DB Type, DB Name, or User Name).
- Note: The Log Full Details Per Session action is not supported for policies that use selective audit trail. Because you are selectively auditing the data, full details are not available.

When a Selective audit trail is enabled for a Guardium security policy:

- If you create a rule on a group of objects, the string on each element in the group is checked. If a match is found, a decision is made to log the information and continue.
- If you create a rule on a group of objects that use a NOT designation on the object group, Guardium still needs to check the string on each element in the group, and decide to log and continue only if none of the elements match. NOT designated rules behave the same as normal rules when used with selective audit trail.

These rules include

- OR situations such as rules based on multiple objects or commands.
- Situations with two NOT conditions (for example, NOT part of a group of objects and NOT part of a group of commands).
- Situations with one NOT condition and one YES condition (for example, a NOT part of a group of objects and a YES part of a group of commands).

Note: Any select statements with query hints, such as `SELECT /*+ ORDERED USE_MERGE(m)`

`*/, SELECT /*+ ORDERED */`, or `SELECT /*+ all_rows */` are allowed to pass through the parser and logged regardless of the rule definition to skip them (at least with selective audit mode). A selective audit policy should not prevent logging of certain SQLs that might be needed for other functions, like application user translation.

## Selective Audit Trail and Application Events API

---

When a selective audit trail policy is used, and application users or events are being set via the Application Events API, the policy must include an Audit Only rule that fires whenever a set/clear application event, or set/clear application user command is encountered. For more information about setting the application user via the Application Events API, see [Identify Users with API](#).

## Selective Audit Trail and Application User Translation

---

When a selective audit trail policy is used, an Application User Translation is also used:

- The policy ignores all of the traffic that does not fit the application user translation rule (for example, not from the application server).
- Only the SQL that matches the pattern for that policy is available for the special application user translation reports.

## Selective Audit Trail and specifying an empty group

---

An empty tuple group attached to a rule does not cause a rule action to match.

## Analyzer rules

---

Certain rules can be applied at the analyzer level.

Examples of analyzer rules are: user-defined character sets, source program changes, and issuing watch verdicts for firewall mode. Rules applied at the analyzer level means decisions can be made at an earlier stage.

## Character sets

---

You can use character set codes in extrusion rules.

## List of possible character set codes

---

ANSI\_X3.4-1968 - 1  
ANSI\_X3.4-1986 - 2  
ASCII - 3  
CP367 - 4  
IBM367 - 5  
ISO-IR-6 - 6  
ISO646-US - 7

ISO\_646.IRV:1991 - 8  
US - 9  
US-ASCII - 10  
CSASCII - 11  
UTF-8 - 12  
ISO-10646/UCS2 - 13  
UCS-2 - 14  
CSUNICODE - 15  
UCS-2BE - 16  
UNICODE - 17  
UNICODEBIG - 18  
TSCII - 19  
UCS-2LE - 20  
UNICODELITTLE - 21  
ISO-10646/UCS4 - 22  
UCS-4 - 23  
CSUCS4 - 24  
UCS-4BE - 25  
UCS-4LE - 26  
UTF-16 - 27  
UTF-16BE - 28  
UTF-16LE - 29  
UTF-32 - 30  
UTF-32BE - 31  
UTF-32LE - 32  
UTF7 - 33  
UTF-7 - 34  
UTF-8 - 35  
UCS2 - 36  
UCS2 - 37  
UCS4 - 38  
UCS4 - 39  
UTF8 - 40  
UTF8 - 41  
CP819 - 42  
IBM819 - 43  
ISO-8859-1 - 44  
ISO-IR-100 - 45  
ISO8859-1 - 46  
ISO\_8859-1 - 47  
ISO\_8859-1:1987 - 48  
L1 - 49  
LATIN1 - 50  
CSISOLATIN1 - 51  
ISO-8859-2 - 52  
ISO-IR-101 - 53  
ISO8859-2 - 54  
ISO\_8859-2 - 55  
ISO\_8859-2:1987 - 56  
L2 - 57  
LATIN2 - 58  
CSISOLATIN2 - 59  
ISO-8859-3 - 60  
ISO-IR-109 - 61  
ISO8859-3 - 62  
ISO\_8859-3 - 63  
ISO\_8859-3:1988 - 64  
L3 - 65  
LATIN3 - 66  
CSISOLATIN3 - 67  
ISO-8859-4 - 68  
ISO-IR-110 - 69  
ISO8859-4 - 70  
ISO\_8859-4 - 71  
ISO\_8859-4:1988 - 72  
L4 - 73  
LATIN4 - 74  
CSISOLATIN4 - 75  
CYRILLIC - 76  
ISO-8859-5 - 77  
ISO-IR-144 - 78  
ISO8859-5 - 79  
ISO\_8859-5 - 80  
ISO\_8859-5:1988 - 81  
CSISOLATINCYRILLIC - 82  
ARABIC - 83  
ASMO-708 - 84  
ECMA-114 - 85  
ISO-8859-6 - 86  
ISO-IR-127 - 87

ISO8859-6 - 88  
ISO\_8859-6 - 89  
ISO\_8859-6:1987 - 90  
CSISOLATINARABIC - 91  
ECMA-118 - 92  
ELOT\_928 - 93  
GREEK - 94  
GREEK8 - 95  
ISO-8859-7 - 96  
ISO-IR-126 - 97  
ISO8859-7 - 98  
ISO\_8859-7 - 99  
ISO\_8859-7:1987 - 100  
CSISOLATINGREEK - 101  
HEBREW - 102  
ISO-8859-8 - 103  
ISO-IR-138 - 104  
ISO8859-8 - 105  
ISO\_8859-8 - 106  
ISO\_8859-8:1988 - 107  
CSISOLATINHEBREW - 108  
ISO-8859-9 - 109  
ISO-IR-148 - 110  
ISO8859-9 - 111  
ISO\_8859-9 - 112  
ISO\_8859-9:1989 - 113  
L5 - 114  
LATIN5 - 115  
CSISOLATIN5 - 116  
ISO-8859-10 - 117  
ISO-IR-157 - 118  
ISO8859-10 - 119  
ISO\_8859-10 - 120  
ISO\_8859-10:1992 - 121  
L6 - 122  
LATIN6 - 123  
CSISOLATIN6 - 124  
ISO-8859-13 - 125  
ISO-8859-13 - 126  
ISO-8859-13 - 127  
ISO-8859-13 - 128  
L7 - 129  
LATIN7 - 130  
ISO-8859-14 - 131  
ISO-CELTIC - 132  
ISO-IR-199 - 133  
ISO8859-14 - 134  
ISO\_8859-14 - 135  
ISO\_8859-14:1998 - 136  
L8 - 137  
LATIN8 - 138  
ISO-8859-15 - 139  
ISO-IR-203 - 140  
ISO8859-15 - 141  
ISO\_8859-15 - 142  
ISO\_8859-15:1998 - 143  
ISO-8859-16 - 144  
ISO-IR-226 - 145  
ISO8859-16 - 146  
ISO\_8859-16 - 147  
ISO\_8859-16:2000 - 148  
KOI8-R - 149  
CSKOI8R? - 150  
KOI8U? - 151  
KOI8R? - 152  
CP1250 - 153  
MS-EE - 154  
WINDOWS-1250 - 155  
CP1251 - 156  
MS-CYRL - 157  
WINDOWS-1251 - 158  
CP1252 - 159  
MS-ANSI - 160  
WINDOWS-1252 - 161  
CP1253 - 162  
MS-GREEK - 163  
WINDOWS-1253 - 164  
CP1254 - 165  
MS-TURK - 166  
WINDOWS-1254 - 167

CP1255 - 168  
MS-HEBR - 169  
WINDOWS-1255 - 170  
CP1256 - 171  
MS-ARAB - 172  
WINDOWS-1256 - 173  
CP1257 - 174  
WINBALTRIM - 175  
WINDOWS-1257 - 176  
CP1258 - 177  
WINDOWS-1258 - 178  
850 - 179  
CP850 - 180  
IBM850 - 181  
CSPC850MULTILINGUAL? - 182  
862 - 183  
CP862 - 184  
IBM862 - 185  
CSPC862LATINHEBREW? - 186  
866 - 187  
CP866 - 188  
IBM866 - 189  
CSIBM866 - 190  
MAC - 191  
MACINTOSH - 192  
MACUK - 193  
CSMACINTOSH - 194  
MACIS - 195  
MAC - 196  
MAC - 197  
MAC - 198  
MAC - 199  
MACUKRAINIAN - 200  
MAC - 201  
MAC - 202  
MAC - 203  
MAC - 204  
MAC - 205  
HP-ROMAN8 - 206  
R8 - 207  
ROMAN8 - 208  
HPROMAN8 - 209  
ROMAN8 - 210  
ARMSCII-8 - 211  
GEORGIAN-ACADEMY - 212  
GEORGIAN-PS - 213  
KOI8-T - 214  
KOI8-T - 215  
CP1133 - 216  
IBM-CP1133 - 217  
ISO-IR-166 - 218  
TIS-620 - 219  
TIS620 - 220  
TIS620-0 - 221  
TIS620.2529-1 - 222  
TIS620.2533-0 - 223  
TIS620.2533-1 - 224  
CP874 - 225  
WINDOWS-874 - 226  
VISCII - 227  
VISCII - 228  
VISCII - 229  
TCVN - 230  
TCVN-5712 - 231  
TCVN5712-1 - 232  
TCVN5712-1:1993 - 233  
ISO-IR-14 - 234  
ISO646-JP - 235  
JIS\_C6220-1969-RO - 236  
JP - 237  
CSISO14JISC6220RO? - 238  
JISX0201-1976 - 239  
JIS\_X0201 - 240  
X0201 - 241  
CSHALFWIDTHKATAKANA - 242  
ISO-IR-87 - 243  
JIS0208 - 244  
JIS\_C6226-1983 - 245  
JIS\_X0208 - 246  
JIS\_X0208-1983 - 247

JIS\_X0208-1990 - 248  
X0208 - 249  
CSISO87JISX0208? - 250  
ISO-IR-159 - 251  
JIS\_X0212 - 252  
JIS\_X0212-1990 - 253  
JIS\_X0212.1990-0 - 254  
X0212 - 255  
CSISO159JISX02121990? - 256  
CN - 257  
GB\_1988-80 - 258  
ISO-IR-57 - 259  
ISO646-CN - 260  
CSISO57GB1988? - 261  
CHINESE - 262  
GB\_2312-80 - 263  
ISO-IR-58 - 264  
CSISO58GB231280? - 265  
CN-GB-ISOIR165 - 266  
ISO-IR-165 - 267  
ISO-IR-149 - 268  
KOREAN - 269  
KSC\_5601 - 270  
KS\_C\_5601-1987 - 271  
KS\_C\_5601-1989 - 272  
CSKSC56011987 - 273  
EUC-JP - 274  
EUCJP - 275  
EXTENDED\_UNIX\_CODE\_PACKED\_FORMAT\_FOR\_JAPANESE - 276  
CSEUCPKDFMTJAPANESE - 277  
MS\_KANJI - 278  
SHIFT-JIS - 279  
SHIFT\_JIS - 280  
SJIS - 281  
CSSHIFTJIS - 282  
CP932 - 283  
ISO-2022-JP - 284  
CSISO2022JP? - 285  
ISO-2022-JP-1 - 286  
ISO-2022-JP-2 - 287  
CSISO2022JP2? - 288  
CN-GB - 289  
EUC-CN - 290  
EUCCN - 291  
GB2312 - 292  
CSGB2312 - 293  
CP936 - 294  
GBK - 295  
GB18030 - 296  
ISO-2022-CN - 297  
CSISO2022CN? - 298  
ISO-2022-CN-EXT - 299  
HZ - 300  
HZ-GB-2312 - 301  
EUC-TW - 302  
EUCTW - 303  
CSEUCTW - 304  
BIG-5 - 305  
BIG-FIVE - 306  
BIG5 - 307  
BIGFIVE - 308  
CN-BIG5 - 309  
CSBIG5 - 310  
CP950 - 311  
BIG5-HKSCS - 312  
BIG5HKSCS? - 313  
EUC-KR - 314  
EUCKR - 315  
CSEUCKR - 316  
CP949 - 317  
UHC - 318  
CP1361 - 319  
JOHAB - 320  
ISO-2022-KR - 321  
CSISO2022KR? - 322  
IBMO37 - 323  
IBMO38 - 324  
IBM256 - 325  
IBM273 - 326  
IBM274 - 327

IBM275 - 328  
IBM277 - 329  
IBM278 - 330  
IBM280 - 331  
IBM281 - 332  
IBM284 - 333  
IBM285 - 334  
IBM290 - 335  
IBM297 - 336  
IBM367 - 337  
IBM420 - 338  
IBM423 - 339  
IBM424 - 340  
IBM437 - 341  
IBM500 - 342  
IBM775 - 343  
IBM813 - 344  
IBM819 - 345  
IBM848 - 346  
IBM850 - 347  
IBM851 - 348  
IBM852 - 349  
IBM855 - 350  
IBM856 - 351  
IBM857 - 352  
IBM860 - 353  
IBM861 - 354  
IBM862 - 355  
IBM863 - 356  
IBM864 - 357  
IBM865 - 358  
IBM866 - 359  
IBM866NAV? - 360  
IBM868 - 361  
IBM869 - 362  
IBM870 - 363  
IBM871 - 364  
IBM874 - 365  
IBM875 - 366  
IBM880 - 367  
IBM891 - 368  
IBM903 - 369  
IBM904 - 370  
IBM905 - 371  
IBM912 - 372  
IBM915 - 373  
IBM916 - 374  
IBM918 - 375  
IBM920 - 376  
IBM922 - 377  
IBM930 - 378  
IBM932 - 379  
IBM933 - 380  
IBM935 - 381  
IBM937 - 382  
IBM939 - 383  
IBM943 - 384  
IBM1004 - 385  
IBM1026 - 386  
IBM1046 - 387  
IBM1047 - 388  
IBM1089 - 389  
IBM1124 - 390  
IBM1129 - 391  
IBM1132 - 392  
IBM1133 - 393  
IBM1160 - 394  
IBM1161 - 395  
IBM1162 - 396  
IBM1163 - 397  
IBM1164 - 398  
MSCP949 - 399  
EUC-JISX0213 - 400  
UJIS - 401  
CP852 - 402  
EUCJP-MS - 403  
IBM902 - 404  
IBM921 - 405  
WINDOWS-31J - 406  
IBM1025 - 407

IBM1140 - 408  
IBM1137 - 409  
IBM1122 - 410  
IBM1141 - 411  
IBM1142 - 412  
IBM1143 - 413  
IBM1144 - 414  
IBM1145 - 415  
IBM1146 - 416  
IBM1147 - 417  
IBM1148 - 418  
IBM1149 - 419  
IBM1153 - 420  
IBM1155 - 421  
IBM1157 - 422  
EBCDICUS - 423  
IBM1112 - 424  
IBM1158 - 425  
437 - 426  
500g - 427  
500V1g - 428  
851g - 429  
852g - 430  
855g - 431  
856g - 432  
857g - 433  
860g - 434  
861g - 435  
863g - 436  
864g - 437  
865g - 438  
866NAvg - 439  
869g - 440  
874g - 441  
904g - 442  
1026g - 443  
1046g - 444  
1047g - 445  
8859\_1g - 446  
8859\_2g - 447  
8859\_3g - 448  
8859\_4g - 449  
8859\_5g - 450  
8859\_6g - 451  
8859\_7g - 452  
8859\_8g - 453  
8859\_9g - 454  
10646-1:1993g - 455  
10646-1:1993/UCS4/ - 456  
ANSI\_X3.4g - 457  
ANSI\_X3.110-1983g - 458  
ANSI\_X3.110g - 459  
ARABIC7g - 460  
ASMO\_449g - 461  
BALTICg - 462  
BIG-5g - 463  
BIG-FIVEg - 464  
BIG5-HKSCSg - 465  
BIG5g - 466  
BIG5HKSCSg? - 467  
BIGFIVEg - 468  
BS\_4730g - 469  
CAG - 470  
CN-BIG5g - 471  
CN-GBg - 472  
CNG - 473  
CP-ARG - 474  
CP-GRg - 475  
CP-HUG - 476  
CP037g - 477  
CP038g - 478  
CP273g - 479  
CP274g - 480  
CP275g - 481  
CP278g - 482  
CP280g - 483  
CP281g - 484  
CP282g - 485  
CP284g - 486  
CP285g - 487

CP290g - 488  
CP297g - 489  
CP420g - 490  
CP423g - 491  
CP424g - 492  
CP437g - 493  
CP500g - 494  
CP737g - 495  
CP775g - 496  
CP803g - 497  
CP813g - 498  
CP851g - 499  
CP852g - 500  
CP855g - 501  
CP856g - 502  
CP857g - 503  
CP860g - 504  
CP861g - 505  
CP863g - 506  
CP864g - 507  
CP865g - 508  
CP866NAVg? - 509  
CP868g - 510  
CP869g - 511  
CP870g - 512  
CP871g - 513  
CP875g - 514  
CP880g - 515  
CP891g - 516  
CP901g - 517  
CP902g - 518  
CP903g - 519  
CP904g - 520  
CP905g - 521  
CP912g - 522  
CP915g - 523  
CP916g - 524  
CP918g - 525  
CP920g - 526  
CP921g - 527  
CP922g - 528  
CP930g - 529  
CP932g - 530  
CP933g - 531  
CP935g - 532  
CP936g - 533  
CP937g - 534  
CP939g - 535  
CP949g - 536  
CP950g - 537  
CP1004g - 538  
CP1008g - 539  
CP1025g - 540  
CP1026g - 541  
CP1046g - 542  
CP1047g - 543  
CP1070g - 544  
CP1079g - 545  
CP1081g - 546  
CP1084g - 547  
CP1089g - 548  
CP1097g - 549  
CP1112g - 550  
CP1122g - 551  
CP1123g - 552  
CP1124g - 553  
CP1125g - 554  
CP1129g - 555  
CP1130g - 556  
CP1132g - 557  
CP1137g - 558  
CP1140g - 559  
CP1141g - 560  
CP1142g - 561  
CP1143g - 562  
CP1144g - 563  
CP1145g - 564  
CP1146g - 565  
CP1147g - 566  
CP1148g - 567

CP1149g - 568  
CP1153g - 569  
CP1154g - 570  
CP1155g - 571  
CP1156g - 572  
CP1157g - 573  
CP1158g - 574  
CP1160g - 575  
CP1161g - 576  
CP1162g - 577  
CP1163g - 578  
CP1164g - 579  
CP1166g - 580  
CP1167g - 581  
CP1361g - 582  
CP1364g - 583  
CP1371g - 584  
CP1388g - 585  
CP1390g - 586  
CP1399g - 587  
CP4517g - 588  
CP4899g - 589  
CP4909g - 590  
CP4971g - 591  
CP5347g - 592  
CP9030g - 593  
CP9066g - 594  
CP9448g - 595  
CP10007g - 596  
CP12712g - 597  
CP16804g - 598  
CP1IBM861g - 599  
CSA7-1g - 600  
CSA7-2g - 601  
CSA\_T500-1983g - 602  
CSA\_T500g - 603  
CSA\_Z2243.4-1985-1g - 604  
CSA\_Z2243.4-1985-2g - 605  
CSA\_Z243.419851g - 606  
CSA\_Z243.419852g - 607  
CSDECMSg - 608  
CSEBCDICATDEg - 609  
CSEBCDICATDEAg - 610  
CSEBCDICCAFrg - 611  
CSEBCDICDKNOg - 612  
CSEBCDICDKNOAg - 613  
CSEBCDICESg - 614  
CSEBCDICESAg - 615  
CSEBCDICESSg - 616  
CSEBCDICFISEg - 617  
CSEBCDICFISEAg - 618  
CSEBCDICFRg - 619  
CSEBCDICITg - 620  
CSEBCDICPTg - 621  
CSEBCDICUKg - 622  
CSEBCDICUSg - 623  
CSEUCKRg - 624  
CSEUCPKDFMTJAPANESEg - 625  
CSGB2312g - 626  
CSIBM037g - 627  
CSIBM038g - 628  
CSIBM273g - 629  
CSIBM274g - 630  
CSIBM275g - 631  
CSIBM277g - 632  
CSIBM278g - 633  
CSIBM280g - 634  
CSIBM281g - 635  
CSIBM284g - 636  
CSIBM285g - 637  
CSIBM290g - 638  
CSIBM297g - 639  
CSIBM420g - 640  
CSIBM423g - 641  
CSIBM424g - 642  
CSIBM500g - 643  
CSIBM803g - 644  
CSIBM851g - 645  
CSIBM855g - 646  
CSIBM856g - 647

CSIBM857g - 648  
CSIBM860g - 649  
CSIBM863g - 650  
CSIBM864g - 651  
CSIBM865g - 652  
CSIBM868g - 653  
CSIBM869g - 654  
CSIBM870g - 655  
CSIBM871g - 656  
CSIBM880g - 657  
CSIBM891g - 658  
CSIBM901g - 659  
CSIBM902g - 660  
CSIBM903g - 661  
CSIBM904g - 662  
CSIBM905g - 663  
CSIBM918g - 664  
CSIBM921g - 665  
CSIBM922g - 666  
CSIBM930g - 667  
CSIBM932g - 668  
CSIBM933g - 669  
CSIBM935g - 670  
CSIBM937g - 671  
CSIBM939g - 672  
CSIBM943g - 673  
CSIBM1008g - 674  
CSIBM1025g - 675  
CSIBM1026g - 676  
CSIBM1097g - 677  
CSIBM1112g - 678  
CSIBM1122g - 679  
CSIBM1123g - 680  
CSIBM1124g - 681  
CSIBM1129g - 682  
CSIBM1130g - 683  
CSIBM1132g - 684  
CSIBM1133g - 685  
CSIBM1137g - 686  
CSIBM1140g - 687  
CSIBM1141g - 688  
CSIBM1142g - 689  
CSIBM1143g - 690  
CSIBM1144g - 691  
CSIBM1145g - 692  
CSIBM1146g - 693  
CSIBM1147g - 694  
CSIBM1148g - 695  
CSIBM1149g - 696  
CSIBM1153g - 697  
CSIBM1154g - 698  
CSIBM1155g - 699  
CSIBM1156g - 700  
CSIBM1157g - 701  
CSIBM1158g - 702  
CSIBM1160g - 703  
CSIBM1161g - 704  
CSIBM1163g - 705  
CSIBM1164g - 706  
CSIBM1166g - 707  
CSIBM1167g - 708  
CSIBM1364g - 709  
CSIBM1371g - 710  
CSIBM1388g - 711  
CSIBM1390g - 712  
CSIBM1399g - 713  
CSIBM4517g - 714  
CSIBM4899g - 715  
CSIBM4909g - 716  
CSIBM4971g - 717  
CSIBM5347g - 718  
CSIBM9030g - 719  
CSIBM9066g - 720  
CSIBM9448g - 721  
CSIBM12712g - 722  
CSIBM16804g - 723  
CSIBM11621162g - 724  
CSISO4UNITEDKINGDOMg? - 725  
CSISO10SWEDISHg? - 726  
CSISO11SWEDISHFORNAMEsg? - 727

CSISO15ITALIANg? - 728  
CSISO16PORTUGESEg? - 729  
CSISO17SPANISHg? - 730  
CSISO18GREEK7OLDg? - 731  
CSISO19LATINGREEKg? - 732  
CSISO21GERMANg? - 733  
CSISO25FRENCHg? - 734  
CSISO27LATINGREEK1g? - 735  
CSISO49INISg? - 736  
CSISO50INIS8g? - 737  
CSISO51INISCYRILLICg? - 738  
CSISO58GB1988g? - 739  
CSISO60DANISHNORWEGIAn? - 740  
CSISO60NORWEGIAN1g? - 741  
CSISO61NORWEGIAN2g? - 742  
CSISO69FRENCHg? - 743  
CSISO84PORTUGUESE2g? - 744  
CSISO85SPANISH2g? - 745  
CSISO86HUNGARIAn? - 746  
CSISO88GREEK7g? - 747  
CSISO89ASMO449g? - 748  
CSISO90g - 749  
CSISO92JISC62991984Bg? - 750  
CSISO99NAPLPSg? - 751  
CSISO103T618BITg? - 752  
CSISO111ECMACYRILLICg? - 753  
CSISO121CANADIAN1g? - 754  
CSISO122CANADIAN2g? - 755  
CSISO139CSN369103g? - 756  
CSISO141JUSIB1002g? - 757  
CSISO143IECP271g? - 758  
CSISO150g - 759  
CSISO150GREEKCCITTg? - 760  
CSISO151CUBAg? - 761  
CSISO153GOST1976874g? - 762  
CSISO646DANISHg? - 763  
CSISO2022CNg? - 764  
CSISO2022JPg? - 765  
CSISO20223JPg? - 766  
CSISO2022KRg? - 767  
CSISO2033g - 768  
CSISO5427CYRILLICg? - 769  
CSISO5427CYRILLIC1981g? - 770  
CSISO5428GREEKg? - 771  
CSISO10367BOXg? - 772  
CSKSC5636g - 773  
CSNATSDANOg - 774  
CSNATSSEF1g - 775  
CSN\_369103g - 776  
CSPC8CODEPAGE437g? - 777  
CSPC775BALТИCg? - 778  
CSPCP852g - 779  
CSSHIFTJISg - 780  
CSUCS4g - 781  
CSWINDOWS31Jg? - 782  
CUBAg - 783  
CWI-2g - 784  
CWIG - 785  
DEg - 786  
DEC-MCSg - 787  
DECg - 788  
DECMCsG - 789  
DIN\_66003g - 790  
DKg - 791  
DS2089g - 792  
DS\_2089g - 793  
E13Bg? - 794  
EBCDIC-AT-DE-Ag - 795  
EBCDIC-AT-DEg - 796  
EBCDIC-BEg - 797  
EBCDIC-BRg - 798  
EBCDIC-CA-FRg - 799  
EBCDIC-CP-AR1g - 800  
EBCDIC-CP-AR2g - 801  
EBCDIC-CP-BEg - 802  
EBCDIC-CP-CAG - 803  
EBCDIC-CP-CHg - 804  
EBCDIC-CP-DKg - 805  
EBCDIC-CP-ESg - 806  
EBCDIC-CP-F1g - 807

EBCDIC-CP-FRg - 808  
EBCDIC-CP-GBg - 809  
EBCDIC-CP-GRg - 810  
EBCDIC-CP-HEg - 811  
EBCDIC-CP-ISg - 812  
EBCDIC-CP-ITg - 813  
EBCDIC-CP-NLg - 814  
EBCDIC-CP-NOg - 815  
EBCDIC-CP-ROECeg - 816  
EBCDIC-CP-SEg - 817  
EBCDIC-CP-TRg - 818  
EBCDIC-CP-USg - 819  
EBCDIC-CP-WTg - 820  
EBCDIC-CP-YUg - 821  
EBCDIC-CYRILLICg - 822  
EBCDIC-DK-NO-Ag - 823  
EBCDIC-DK-NOg - 824  
EBCDIC-ES-Ag - 825  
EBCDIC-ES-Sg - 826  
EBCDIC-ESg - 827  
EBCDIC-FI-SE-Ag - 828  
EBCDIC-FI-SEG - 829  
EBCDIC-FRg - 830  
EBCDIC-GREEKg - 831  
EBCDIC-INTg - 832  
EBCDIC-INT1g - 833  
EBCDIC-IS-FRISSg - 834  
EBCDIC-ITg - 835  
EBCDIC-JP-Eg - 836  
EBCDIC-JP-KANAg - 837  
EBCDIC-PTg - 838  
EBCDIC-UKg - 839  
EBCDIC-USg - 840  
EBCDICATDEg - 841  
EBCDICATDEAg - 842  
EBCDICCAFRg - 843  
EBCDICDKNOg - 844  
EBCDICDKNOAg - 845  
EBCDICESg - 846  
EBCDICESAg - 847  
EBCDICESSg - 848  
EBCDICFISEg - 849  
EBCDICFISEAg - 850  
EBCDICFRg - 851  
EBCDICISFRISSg - 852  
EBCDICITg - 853  
EBCDICPTg - 854  
EBCDICUKg - 855  
EBCDICUSg - 856  
ECMA-128g - 857  
ECMA-CYRILLICg - 858  
ECMACYRILLICg - 859  
ESg - 860  
ES2g - 861  
EUC-CNG - 862  
EUC-JISX0213g - 863  
EUC-JP-MSg - 864  
EUC-JPg - 865  
EUC-KRg - 866  
EUC-TWg - 867  
EUCCNG - 868  
EUCJP-MSg - 869  
EUCJP-OPENg - 870  
EUCJP-WINg - 871  
EUCJPg - 872  
EUCKRg - 873  
EUCTWg - 874  
FIg - 875  
FRg - 876  
GBg - 877  
GB2312g - 878  
GB13000g - 879  
GB18030g - 880  
GBKg - 881  
GB\_1988-80g - 882  
GB\_198880g - 883  
GOST\_19768-74g - 884  
GOST\_19768g - 885  
GOST\_1976874g - 886  
GREEK-CCITTg - 887

GREEK7-OLDg - 888  
GREEK7g - 889  
GREEK7OLDg? - 890  
GREEKCCITTg - 891  
HUG - 892  
IBM-803g - 893  
IBM-856g - 894  
IBM-901g - 895  
IBM-902g - 896  
IBM-921g - 897  
IBM-922g - 898  
IBM-930g - 899  
IBM-932g - 900  
IBM-933g - 901  
IBM-935g - 902  
IBM-937g - 903  
IBM-939g - 904  
IBM-943g - 905  
IBM-1008g - 906  
IBM-1025g - 907  
IBM-1046g - 908  
IBM-1047g - 909  
IBM-1097g - 910  
IBM-1112g - 911  
IBM-1122g - 912  
IBM-1123g - 913  
IBM-1124g - 914  
IBM-1129g - 915  
IBM-1130g - 916  
IBM-1132g - 917  
IBM-1133g - 918  
IBM-1137g - 919  
IBM-1140g - 920  
IBM-1141g - 921  
IBM-1142g - 922  
IBM-1143g - 923  
IBM-1144g - 924  
IBM-1145g - 925  
IBM-1146g - 926  
IBM-1147g - 927  
IBM-1148g - 928  
IBM-1149g - 929  
IBM-1153g - 930  
IBM-1154g - 931  
IBM-1155g - 932  
IBM-1156g - 933  
IBM-1157g - 934  
IBM-1158g - 935  
IBM-1160g - 936  
IBM-1161g - 937  
IBM-1162g - 938  
IBM-1163g - 939  
IBM-1164g - 940  
IBM-1166g - 941  
IBM-1167g - 942  
IBM-1364g - 943  
IBM-1371g - 944  
IBM-1388g - 945  
IBM-1390g - 946  
IBM-1399g - 947  
IBM-4517g - 948  
IBM-4899g - 949  
IBM-4909g - 950  
IBM-4971g - 951  
IBM-5347g - 952  
IBM-9030g - 953  
IBM-9066g - 954  
IBM-9448g - 955  
IBM-12712g - 956  
IBM-16804g - 957  
IBM037g - 958  
IBM038g - 959  
IBM256g - 960  
IBM273g - 961  
IBM274g - 962  
IBM275g - 963  
IBM277g - 964  
IBM278g - 965  
IBM280g - 966  
IBM281g - 967

IBM284g - 968  
IBM285g - 969  
IBM290g - 970  
IBM297g - 971  
IBM420g - 972  
IBM423g - 973  
IBM424g - 974  
IBM437g - 975  
IBM500g - 976  
IBM775g - 977  
IBM803g - 978  
IBM813g - 979  
IBM848g - 980  
IBM851g - 981  
IBM852g - 982  
IBM855g - 983  
IBM856g - 984  
IBM857g - 985  
IBM860g - 986  
IBM861g - 987  
IBM863g - 988  
IBM864g - 989  
IBM865g - 990  
IBM866NAVg? - 991  
IBM868g - 992  
IBM869g - 993  
IBM870g - 994  
IBM871g - 995  
IBM874g - 996  
IBM875g - 997  
IBM880g - 998  
IBM891g - 999  
IBM901g - 1000  
IBM902g - 1001  
IBM903g - 1002  
IBM904g - 1003  
IBM905g - 1004  
IBM912g - 1005  
IBM915g - 1006  
IBM916g - 1007  
IBM918g - 1008  
IBM920g - 1009  
IBM921g - 1010  
IBM922g - 1011  
IBM930g - 1012  
IBM932g - 1013  
IBM933g - 1014  
IBM935g - 1015  
IBM937g - 1016  
IBM939g - 1017  
IBM943g - 1018  
IBM1004g - 1019  
IBM1008g - 1020  
IBM1025g - 1021  
IBM1026g - 1022  
IBM1046g - 1023  
IBM1047g - 1024  
IBM1089g - 1025  
IBM1097g - 1026  
IBM1112g - 1027  
IBM1122g - 1028  
IBM1123g - 1029  
IBM1124g - 1030  
IBM1129g - 1031  
IBM1130g - 1032  
IBM1132g - 1033  
IBM1133g - 1034  
IBM1137g - 1035  
IBM1140g - 1036  
IBM1141g - 1037  
IBM1142g - 1038  
IBM1143g - 1039  
IBM1144g - 1040  
IBM1145g - 1041  
IBM1146g - 1042  
IBM1147g - 1043  
IBM1148g - 1044  
IBM1149g - 1045  
IBM1153g - 1046  
IBM1154g - 1047

IBM1155g - 1048  
IBM1156g - 1049  
IBM1157g - 1050  
IBM1158g - 1051  
IBM1160g - 1052  
IBM1161g - 1053  
IBM1162g - 1054  
IBM1163g - 1055  
IBM1164g - 1056  
IBM1166g - 1057  
IBM1167g - 1058  
IBM1364g - 1059  
IBM1371g - 1060  
IBM1388g - 1061  
IBM1390g - 1062  
IBM1399g - 1063  
IBM4517g - 1064  
IBM4899g - 1065  
IBM4909g - 1066  
IBM4971g - 1067  
IBM5347g - 1068  
IBM9030g - 1069  
IBM9066g - 1070  
IBM9448g - 1071  
IBM12712g - 1072  
IBM16804g - 1073  
IEC\_P27-1g - 1074  
IEC\_P271g - 1075  
INIS-8g - 1076  
INIS-CYRILLICg - 1077  
INISg - 1078  
INIS8g - 1079  
INISCYRILLICg - 1080  
ISIRI-3342g - 1081  
ISIRI3342g - 1082  
ISO-2022-CN-EXTg - 1083  
ISO-2022-CNg - 1084  
ISO-2022-JP-2g - 1085  
ISO-2022-JP-3g - 1086  
ISO-2022-JPg - 1087  
ISO-2022-KRg - 1088  
ISO-8859-9g - 1089  
ISO-8859-10g - 1090  
ISO-8859-11g - 1091  
ISO-8859-16g - 1092  
ISO-10646g - 1093  
ISO-10646=UTF-8/- 1094  
ISO-10646=UTF8/- 1095  
ISO-IR-4g - 1096  
ISO-IR-8-1g - 1097  
ISO-IR-9-1g - 1098  
ISO-IR-10g - 1099  
ISO-IR-11g - 1100  
ISO-IR-15g - 1101  
ISO-IR-16g - 1102  
ISO-IR-17g - 1103  
ISO-IR-18g - 1104  
ISO-IR-19g - 1105  
ISO-IR-21g - 1106  
ISO-IR-25g - 1107  
ISO-IR-27g - 1108  
ISO-IR-37g - 1109  
ISO-IR-49g - 1110  
ISO-IR-50g - 1111  
ISO-IR-51g - 1112  
ISO-IR-54g - 1113  
ISO-IR-55g - 1114  
ISO-IR-57g - 1115  
ISO-IR-60g - 1116  
ISO-IR-61g - 1117  
ISO-IR-69g - 1118  
ISO-IR-84g - 1119  
ISO-IR-85g - 1120  
ISO-IR-86g - 1121  
ISO-IR-88g - 1122  
ISO-IR-89g - 1123  
ISO-IR-90g - 1124  
ISO-IR-92g - 1125  
ISO-IR-98g - 1126  
ISO-IR-99g - 1127

ISO-IR-103g - 1128  
ISO-IR-111g - 1129  
ISO-IR-121g - 1130  
ISO-IR-122g - 1131  
ISO-IR-127g - 1132  
ISO-IR-139g - 1133  
ISO-IR-141g - 1134  
ISO-IR-143g - 1135  
ISO-IR-150g - 1136  
ISO-IR-151g - 1137  
ISO-IR-153g - 1138  
ISO-IR-155g - 1139  
ISO-IR-156g - 1140  
ISO-IR-166g - 1141  
ISO-IR-193g - 1142  
ISO-IR-197g - 1143  
ISO-IR-209g - 1144  
ISO/TR\_11548-1/- 1145  
ISO646-CAg - 1146  
ISO646-CA2g - 1147  
ISO646-CNg - 1148  
ISO646-CUg - 1149  
ISO646-DEg - 1150  
ISO646-DKg - 1151  
ISO646-ESg - 1152  
ISO646-ES2g - 1153  
ISO646-FIg - 1154  
ISO646-FRg - 1155  
ISO646-FR1g - 1156  
ISO646-GBg - 1157  
ISO646-HUg - 1158  
ISO646-ITg - 1159  
ISO646-JP-OCR-Bg - 1160  
ISO646-KRg - 1161  
ISO646-NOg - 1162  
ISO646-NO2g - 1163  
ISO646-PTg - 1164  
ISO646-PT2g - 1165  
ISO646-SEg - 1166  
ISO646-SE2g - 1167  
ISO646-YUg - 1168  
ISO2022CNg? - 1169  
ISO2022CNEXTg? - 1170  
ISO2022JPg? - 1171  
ISO2022JP2g? - 1172  
ISO2022KRg? - 1173  
ISO6937g - 1174  
ISO8859-11g - 1175  
ISO11548-1g - 1176  
ISO88591g - 1177  
ISO88592g - 1178  
ISO88593g - 1179  
ISO88594g - 1180  
ISO88595g - 1181  
ISO88596g - 1182  
ISO88597g - 1183  
ISO88598g - 1184  
ISO88599g - 1185  
ISO885910g - 1186  
ISO885911g - 1187  
ISO885913g - 1188  
ISO885914g - 1189  
ISO885915g - 1190  
ISO885916g - 1191  
ISO\_2033-1983g - 1192  
ISO\_2033g - 1193  
ISO\_5427-EXTg - 1194  
ISO\_5427g - 1195  
ISO\_5427:1981g - 1196  
ISO\_5427EXTg - 1197  
ISO\_5428g - 1198  
ISO\_5428:1980g - 1199  
ISO\_6937-2g - 1200  
ISO\_6937-2:1983g - 1201  
ISO\_6937g - 1202  
ISO\_6937:1992g - 1203  
ISO\_8859-7:2003g - 1204  
ISO\_8859-16:2001g - 1205  
ISO\_9036g - 1206  
ISO\_10367-BOXg - 1207

ISO\_10367BOXg - 1208  
ISO\_11548-1g - 1209  
ISO\_69372g - 1210  
ITg - 1211  
JIS\_C6229-1984-Bg - 1212  
JIS\_O62201969ROg - 1213  
JIS\_C62291984Bg - 1214  
JOHABg - 1215  
JP-OCR-Bg - 1216  
JSg - 1217  
JUS\_I.B1.002g - 1218  
KOI-7g - 1219  
KOI-8g - 1220  
KOI8g - 1221  
KSC5636g - 1222  
L10g - 1223  
LATIN-9g - 1224  
LATIN-GREEK-1g - 1225  
LATIN-GREEKg - 1226  
LATIN10g - 1227  
LATINGREEKg - 1228  
LATINGREEK1g - 1229  
MAC-CYRILLICg - 1230  
MAC-ISg - 1231  
MAC-SAM1g - 1232  
MAC-UKg - 1233  
MACCYRILLICg - 1234  
MIKg - 1235  
MS-MAC-CYRILLICg - 1236  
MS932g - 1237  
MS936g - 1238  
MSCP949g - 1239  
MSCP1361g - 1240  
MSMACCYRILLICg - 1241  
MSZ\_7795.3g - 1242  
MS\_KANJ1g - 1243  
NAPLPSg - 1244  
NATS-DANOg - 1245  
NATS-SEFIg - 1246  
NATSDANOg - 1247  
NATSSEFIg - 1248  
NC\_NC0010g - 1249  
NC\_NC00-10g - 1250  
NC\_NC00-10:81g - 1251  
NF\_Z\_62-010g - 1252  
NF\_Z\_62-010\_(1973)g - 1253  
NF\_Z\_62-010\_1973g - 1254  
NF\_Z\_62010g - 1255  
NF\_Z\_62010\_1973g - 1256  
NOg - 1257  
NO2g - 1258  
NS\_4551-1g - 1259  
NS\_4551-2g - 1260  
NS\_45511g - 1261  
NS\_45512g - 1262  
OS2LATIN1g? - 1263  
OSF00010001g - 1264  
OSF00010002g - 1265  
OSF00010003g - 1266  
OSF00010004g - 1267  
OSF00010005g - 1268  
OSF00010006g - 1269  
OSF00010007g - 1270  
OSF00010008g - 1271  
OSF00010009g - 1272  
OSF0001000A? - 1273  
OSF00010020g - 1274  
OSF00010100g - 1275  
OSF00010101g - 1276  
OSF00010102g - 1277  
OSF00010104g - 1278  
OSF00010105g - 1279  
OSF00010106g - 1280  
OSF00030010g - 1281  
OSF0004000Ag? - 1282  
OSF0005000Ag? - 1283  
OSF05010001g - 1284  
OSF100201A4g? - 1285  
OSF100201A8g? - 1286  
OSF100201B5g? - 1287

OSF100201F4g? - 1288  
OSF100203B5g? - 1289  
OSF1002011Cg? - 1290  
OSF1002011Dg? - 1291  
OSF1002035Dg? - 1292  
OSF1002035Eg? - 1293  
OSF1002035Fg? - 1294  
OSF1002036Bg? - 1295  
OSF1002037Bg? - 1296  
OSF10010001g - 1297  
OSF10020025g - 1298  
OSF10020111g - 1299  
OSF10020115g - 1300  
OSF10020116g - 1301  
OSF10020118g - 1302  
OSF10020122g - 1303  
OSF10020129g - 1304  
OSF10020352g - 1305  
OSF10020354g - 1306  
OSF10020357g - 1307  
OSF10020359g - 1308  
OSF10020360g - 1309  
OSF10020364g - 1310  
OSF10020365g - 1311  
OSF10020366g - 1312  
OSF10020367g - 1313  
OSF10020370g - 1314  
OSF10020387g - 1315  
OSF10020388g - 1316  
OSF10020396g - 1317  
OSF10020402g - 1318  
OSF10020417g - 1319  
PTg - 1320  
PT2g - 1321  
PT154g - 1322  
RK1048g - 1323  
RUSCI Ig - 1324  
SEg - 1325  
SE2g - 1326  
SEN\_850200\_Bg - 1327  
SEN\_850200\_Cg - 1328  
SHIFT-JISg - 1329  
SHIFT\_JISg - 1330  
SHIFT\_JISX0213g - 1331  
SJIS-OPENg - 1332  
SJIS-WINg - 1333  
SJISg - 1334  
SS636127g - 1335  
STRK1048-2002g - 1336  
ST\_SEV\_358-88g - 1337  
T.61-8BITg - 1338  
T.61g - 1339  
T.618BITg - 1340  
TS-5881g - 1341  
UHCg - 1342  
UJISg - 1343  
UKg - 1344  
UTF8g - 1345  
UTF16g - 1346  
UTF16BEg? - 1347  
UTF16LEg? - 1348  
UTF32g - 1349  
UTF32BEg? - 1350  
UTF32LEg? - 1351  
WCHAR\_Tg - 1352  
WIN-SAMI-2g - 1353  
WINDOWS-31Jg - 1354  
WINDOWS-936g - 1355  
WINSAMI2g - 1356  
WS2g - 1357  
YUg - 1358

---

## Session-level policies

Session-level policies and advanced session-level policies create new possibilities for detecting suspicious behavior of users of services as well as security incidents. Session-level policies are created using the Policy Builder for Data, and advanced session level policies are created as scripts using the SR language and uploaded to Guardium using the Policy Builder for Data.

Session-level policies create new possibilities for detecting suspicious service user behavior as well as security incidents. Session-level policies can detect issues such as credential stuffing, denial of service (DoS) attacks, password spraying attacks, data exfiltration, and administrative security breaches. Session-level policies include machine learning algorithms for security anomaly detection. Use session-level policy rules to effectively tailor analyzed traffic for security processing and information event management (SIEM) in real time, and evaluate the level of session trust.

The quality of a security system depends on its ability to detect suspicious behavior of service users. As Data Security Standards (DSS) and Data Protection Regulations (DPR) are updated and become more stringent, session-level policies cover important data security requirements.

Employing session-level policies is the first phase in checking the security of incoming network traffic. The policies act based on the outcome of the security check. Various types of actions are available. For example, an action might terminate the offending connection, make data transformations that are useful for reporting, or alert and warn of various security violations.

Multiple session-level policies can be used at the same time, which is installed in a user-defined order. Each session-level policy can contain multiple rules. Rules are sets of conditions with one or more associated actions. Session-level policies can be imported, exported, and managed both locally and from a central manager.

Guardium provides a number of session-level policies from the Policy Builder for Data page. Policies are in the form of templates; you can view templates, but you cannot change them. To create a session-level policy to meet your requirements, you can either create a new policy, or copy an existing template, as described in [Creating session-level policies](#).

- [Creating session-level and advanced session-level policies](#)

Learn how to create and install session-level and advanced session-level policies.

- [Using session-level and advanced session-level policies](#)

Use session-level policies or advanced session-level policy scripts to validate incoming packets and define actions based on the result. This guide describes the criteria, actions, and other elements available for creating session level policies and advanced session level policies.

- [Criteria](#)

- [Tuples](#)

- [Actions](#)

- [Action parameters](#)

- [Session-level policy examples](#)

To help you understand session-level policies, Guardium provides a number of examples with descriptions. The examples include both the Guardium UI and SR language methods.

- [Known limitations](#)

The following known limitations apply to session-level policies and advanced session-level policies.

## Creating session-level and advanced session-level policies

Learn how to create and install session-level and advanced session-level policies.

- [Creating session-level policies](#)

Use the Policy Builder for Data to create and install session-level policies.

- [Creating advanced session-level policies](#)

Use advanced session-level policy scripts to validate incoming packets and define actions based on the result. The action can send the request back to the S-TAP, transform the runtime data for the analyzer, and prepare the data for the parser or logger.

## Creating session-level policies

Use the Policy Builder for Data to create and install session-level policies.

### About this task

The overall workflow for defining session-level policies is the same as for standard data-security policies. For information about defining policies, see [Creating and installing a policy and policy rules](#). This procedure focuses on unique aspects of creating session-level policies.

### Procedure

1. Navigate to Protect > Security Policies > Policy Builder for Data.
2. Create a new policy or clone an existing policy.

- To create a new policy, click the  icon.

- To clone a policy, select an existing session level policy template from the Security Policies window and then click the  icon.

- Important: Policies that are installed from the central manager to an aggregator might appear in the aggregator UI as not installed because you cannot install policies on an aggregator. To determine whether a policy is installed, run the [list\\_installed\\_policies](#) API or check in the Policy Builder for Data page for each aggregator.

The Create New Policy window displays.

3. For a new policy, from the Name and properties pane, set the policy type to Session level policy and define a policy name.

Attention: After a policy is saved as a session-level policy, you cannot change it to a data-security policy.

4. Click the Rules pane to begin working with policy rules, then create a new rule by clicking the  icon.

- a. From the Rule definition pane of the Create New Rule window, define a Rule name.

For session-level policies, the Rule type field is predefined to Session.

- b. Click the Rule criteria pane and begin defining rule parameters and values.

- Use the menus to select individual parameters and define selection operators, and then specify values or groups to match.

- Use the  and  icons to add or remove criteria from the rule.

For more information about rule criteria, see [Rule definition fields](#) and [Values and groups of values in rules](#)

Attention: Unlike standard data-security policies, all rule criteria available for session-level policies are based on the session.

- c. Click the Rule action pane to begin working with rule actions, then create a new rule action by clicking the  icon and selecting an action. If further configuration is necessary, use the Add New Action window to define the action. For more information about available actions, see the [Actions](#) section of the [Using session-level and advanced session-level policies](#).
- d. When finished defining the rule, click OK to return to the Rules pane.  
Continue working with rules as needed.

5. When finished defining the policy and its rules, click OK to save the policy and return to the Security Policies table.

## What to do next

Install policies by selecting a policy from the Security Policies window and clicking  Install. Select the Installation action you want and click OK to install the policy.

Installed policies are indicated by a  in the Installed column.

- [Creating tuple parameters for session-level policies](#)

Combine several session-level policy parameters into a single parameter known as a tuple. Compared to using multiple single parameters, where each parameter matches any value in a group, tuple parameters allow finer control by defining only specific combinations of values to match.

## Creating tuple parameters for session-level policies

Combine several session-level policy parameters into a single parameter known as a tuple. Compared to using multiple single parameters, where each parameter matches any value in a group, tuple parameters allow finer control by defining only specific combinations of values to match.

### Before you begin

Create or edit a session-level policy using the Policy Builder for Data, and begin creating or editing a policy rule. This procedure begins with either the Create New Rule or Edit Rule window open.

### Procedure

1. From the Rule criteria panel, select Tuples from the Session level criteria menu.
2. Define a new group or select and edit an existing group to use with the tuple.
  - To define a new group:
    - Use the  icon to open the Create new group dialog.
    - Use the Description field to provide a name for the group.
    - Use the General tab to configure the group. For more information, see [Using the group builder](#).
    - Use the Tuple parameters menu to select parameters to include in the tuple. Use the  icon to specify the tuple order.
  - To edit an existing group, select the group from the menu and use the  icon to open the Edit group dialog. If you do not need to edit the existing group, simply select it and continue defining criteria for the session-level policy.
3. Select the Members tab to populate and work with group members.  
Use the , , and  icons to add, edit, or remove group members. When adding members, the Add member dialog displays fields matching the tuple criteria.  
Note:  
An empty member matches any value. Use GUARDIUM://empty to match an empty value.

## Creating advanced session-level policies

Use advanced session-level policy scripts to validate incoming packets and define actions based on the result. The action can send the request back to the S-TAP, transform the runtime data for the analyzer, and prepare the data for the parser or logger.

### About this task

This procedure describes how to install advanced session-level policies from the Policy Builder for Data. It assumes that you are familiar with creating advanced session-level policies using the SR language or have completed SR scripts ready to import.

### Procedure

1. Open Protect  Security Policies  Policy Builder for Data.
2. Use the  icon to create a new policy.
3. From the Create New Policy window, set the Type to Advanced session level policy and enter a Name for the new policy.
4. Optional: Use the Roles button to assign roles to the policy.
5. Open the Rule panel.
6. Edit or import an advanced session-level policies script.
  - Edit a script:
    - Use the  icon to begin editing an advanced session-level policies script.
    - Use the Check syntax button at any time to validate the script.
    - When you have finished editing the script, click OK.
  - Import a script:
    - Use the Import from file button to open the Select an advanced session level policies script to upload dialog.

- Use the Browse button and select a file to upload. The script file should be plain text and include a valid advanced session level policies script.
  - Use the Upload button to import the script. If there is an existing script, either Append the new script or Replace the existing scripts.
  - You can continue editing the script directly in the Guardium UI. Use the Check syntax button at any time to validate the script.
  - When you have finished editing the script, click OK.
7. If the script validates, the policy is saved and can be installed from the Security Policies table. If the script fails to validate, review the error message and update the script.
- 

## Using session-level and advanced session-level policies

Use session-level policies or advanced session-level policy scripts to validate incoming packets and define actions based on the result. This guide describes the criteria, actions, and other elements available for creating session level policies and advanced session level policies.

In the SR language examples, you can map the parameters (that is, parameter = *variable*) directly to most UI examples. Take for example the following SR language snippet:

```
SR_POLICIES
{
 IF (CLIENT_IP = '10.10.10.10' SOURCE_PROGRAM = 'JAVA%' SERVER_IP = '20.20.20.20')
 {
 IGNORE_SESSION
 }
 IF (*)
 {
 IGNORE_SESSION PACKETS_LIMIT = 50
 }
}
```

- CLIENT\_IP criteria in the SR language maps to Client IP address in the UI
- SERVER\_IP maps to Server IP address.
- SOURCE\_PROGRAM maps to Source application.

In addition, the { IGNORE\_SESSION } code in the SR language maps to the IGNORE SESSION rule action in the UI.

In this guide, you can find the mappings between the SR language and UI elements.

In the guide, the UI name is generally on the left, and the SR language name is on the right. The SR language name is shown in parentheses. For example, looking at search parameters:

Request types available for actions with search parameters:

```
LOGIN FAILED (LOGIN_FAILED)
PREPARED STATEMENT (PREP_STAT)
RPC (RPC)
SQL (SQL)
SQL ERROR (SQL_ERROR)
SQL SUCCESS (SQL_SUCCESS)
```

LOGIN FAILED in the UI maps to LOGIN\_FAILED in the SR language, PREPARED STATEMENT in the UI maps to PREP\_STAT in the SR language.

- [Wildcards](#)
- [Tokens](#)  
Tokens expand to the values of the token name for the current session.
- [IPv6 support](#)  
Session-level and advanced session-level policies support both IPv4 and IPv6 addresses. Any IPv6 notation is supported.
- [Groups](#)  
Groups are combinations of parameters that can be used in rule conditions.
- [Grammar](#)  
Overall syntax and grammar used for creating advanced session-level policies.
- [Unsupported databases for session-level policies](#)

## Wildcards

Session-level policies and the SR language support wildcards:

- % matches zero or more characters
- ? matches a single character

The % wildcard is slower than the ? wildcard.

Wildcards are allowed for the following parameters:

- Groups
- Session-level criteria
- Search pattern (SEARCH\_PATTERN)
- Search prefix (SEARCH\_PREFIX)
- Tuples

This example has the following rule and rule actions, and uses wildcards for session-level criteria.

- Session level criteria
  - Database type = ORA%
  - Database user = ?SCOTTt%
  - Client host name = rh7u6x64t.%

- Rule action
  1. *TRANSFORM SOURCE PROGRAM NAME*
    - Source = *SOURCE PROGRAM NAME*
    - Search prefix = *SQL PLUS*
    - Output format = *PEREL\_PROGRAM*
  2. *DISCARD SESSION*
    - a. Request type = *SQL*
    - b. Search prefix = *SYSTEM*

SR Language example:

```
SR_POLICIES
{
 IF (DB_TYPE = 'ORA%' DB_USER = '?COTT%' CLIENT_HOST_NAME = 'rh7u6x64t.%')
 {
 TRANSFORM_SOURCE_PROGRAM SEARCH_PREFIX = 'SQLPLUS' OUTPUT_FORMAT = 'PEREL_PROGRAM'
 DISCARD_SESSION REQ_TYPE = SQL SEARCH_PATTERN = 'SYSTEM'
 }
}
```

The following values match:

- **DB\_TYPE** matches ORACLE
- **DB\_USER** matches SCOTT
- **CLIENT\_HOST\_NAME** matches rh7u6x64t.domain.name.com

## Tokens

Tokens expand to the values of the token name for the current session.

Supported tokens:

- \$(ACTUAL\_CLIENT\_IP)\$
- \$(ANALYZED\_CLIENT\_IP)\$
- \$(AUTH\_TYPE)\$
- \$(CLIENT\_HOST\_NAME)\$
- \$(CLIENT\_OS\_NAME)\$
- \$(CLIENT\_IP)\$
- \$(CLOGIN\_FAILURES)\$
- \$(COMMAD)\$
- 12.1 and later \$(COLLECTOR\_HOST\_NAME)\$
- \$(CSESSIONS)\$
- \$(CTIMEZONE)\$
- \$(DATETIME)\$
- \$(DB\_NAME)\$
- \$(DB\_TYPE)\$
- \$(DB\_USER)\$
- \$(ERROR)\$
- \$(NET\_PROTOCOL)\$
- \$(OS\_USER)\$
- \$(PE\_EXCEPTION)\$
- \$(SENDER\_IP)\$
- \$(SERVER\_DESCRIPTION)\$
- \$(SERVER\_HOST\_NAME)\$
- \$(SERVER\_IP)\$
- \$(SERVER\_OS\_NAME)\$
- \$(SERVICE\_NAME)\$
- \$(SESSION\_INFO)\$ (return format: client\_ip:client\_port <-> server\_ip:server\_port)
- 12.1 and later \$(SESSION\_KEY)\$
- \$(SOURCE\_PROGRAM)\$
- 12.1 and later \$(STATEMENT\_KEY)\$

Tokens are allowed in:

- Exception message (EXC\_MSG)
- Output format (OUTPUT\_FORMAT)
- Search pattern (SEARCH\_PATTERN)
- Search prefix (SEARCH\_PREFIX)

Example:session\_level\_policies\_actions\_transform

```
SR_POLICIES
{
 IF(OS_USER = 'SALLY')
 {
 TRANSFORM_OS_USER SOURCE = CLIENT_HOST_NAME SEARCH_PATTERN = '$(SERVER_HOST_NAME)$' OUTPUT_FORMAT = (DB_USER)
 }
}
```

If CLIENT\_HOST\_NAME is the same as SERVER\_HOST\_NAME, replace OS\_USER with DB\_USER only when OS\_USER = 'SALLY'.

## IPv6 support

Session-level and advanced session-level policies support both IPv4 and IPv6 addresses. Any IPv6 notation is supported.

Example:

```
SR_POLICIES
{
 IF (CLIENT_IP = '::ffff:150.49.108.36')
 {
 TRANSFORM_SOURCE_PROGRAM MATCH_PATTERN = '^.*$' OUTPUT_FORMAT = 'SPECIAL JDBC'
 }
}

SR_POLICIES
{
 IF (CLIENT_IP = '150.49.108.36')
 {
 TRANSFORM_SOURCE_PROGRAM MATCH_PATTERN = '^.*$' OUTPUT_FORMAT = 'SPECIAL JDBC'
 }
}
```

This shows two logically equal rule conditions using IPv6 and IPv4 notation.

Example:

```
SR_POLICIES
{
 IF (SERVER_IP = ('',1) SERVER_PORT = 1521)
 {
 TRANSFORM_SOURCE_PROGRAM MATCH_PATTERN = '^.*$' OUTPUT_FORMAT = 'SPECIAL JDBC'
 }

 GROUP_ID = 1 TYPE = IP_ADDRESS SIZE = 2 #CLIENT_IP GROUP
 {
 '150.49.108.36' '2002:920:C000:3146::6'
 }
}
```

This example shows a policy for a database server with dual IPv4 and IPv6 addresses.

Example:

```
SR_POLICIES
{
 IF (CLIENT_IP = '::FFFF:DCCC:ED91' CLIENT_NET_MASK = '::FFFF:DCCC:0000' SENDER_IP = '2002:920:C000:3146::6')
 {
 TRANSFORM_OS_USER MATCH_PATTERN = '^.*$' OUTPUT_FORMAT = 'SPECIAL OS_USER'
 }
}
```

This shows how network masks for IPv6 addresses are supported in a format similar to IPv4.

Example:

```
SR_POLICIES
{
 IF (CLIENT_IP = '0.0.0.0' SERVER_IP = '9.70.157.177' ANALYZED_CLIENT_IP = '9.70.144.184' ANALYZED_CLIENT_NET_MASK = '255.255.255.0')
 {
 TRANSFORM_SERVER_DESC SEARCH_PREFIX = '9.' SOURCE = ANALYZED_CLIENT_IP OUTPUT_FORMAT = '(.*)'
 }
}

SR_POLICIES
{
 IF (CLIENT_IP = '0.0.0.0' SERVER_IP = '9.70.157.177' ANALYZED_CLIENT_IP = '::ffff:9.70.144.184' ANALYZED_CLIENT_NET_MASK = '::ffff:0000:0000')
 {
 TRANSFORM_SERVER_DESC SEARCH_PREFIX = '9.' SOURCE = ANALYZED_CLIENT_IP OUTPUT_FORMAT = '(.*)'
 }
}
```

This shows using ANALYZED\_CLIENT\_IP as condition with IPv4 and IPv6 addresses. The rule copies the value from the column ANALYZED\_CLIENT\_IP into the column SERVER\_DESC of table GDM\_ACCESS.

## Groups

Groups are combinations of parameters that can be used in rule conditions.

Multiple groups can be used in one rule.

Session level policy groups are defined like any other policy group using the Policy builder for data.

Advanced session-level policy groups are defined using the SR language as shown in the following examples.

Note:

- To specify a group within the policy, include one element of the group followed by the group ID. In the following example, `admin` is one of the elements in group 1. Specify the remaining group elements at the end of the policy.
- Group contents are always put at the end of policy snippets.

Example:

```
SR_POLICIES
{
 IF (DB_USER != ('admin',1) { VERDICT_ATTACH }

 GROUP_ID = 1 SIZE = 3 { 'root' 'sys' 'system' }
}
```

In this example, the condition includes `DB_USER`, `admin`, and all users from `GROUP_ID = 1`. Here `IF(*)` represents no condition

Example:

```
SR_POLICIES
{
 IF (CLIENT_IP != '192.168.0.1' DB_USER = 'SCOTT') { VERDICT_ATTACH SELECT_SESSION }

 IF (CLIENT_IP != ('192.168.0.2',176) DB_USER = 'SCOTT') { VERDICT_DETACH }

 IF (CLIENT_IP != '192.168.0.3' DB_USER = ('',177) { VERDICT_TERMINATE }

 IF (*) { IGNORE_SESSION_PACKETS_LIMIT = 30 }
 IF (*) { TRANSFORM_SOURCE_PROGRAM MATCH_PATTERN = '' OUTPUT_FORMAT = 'SPECIAL JDBC' }

 GROUP_ID = 176 TYPE = IP_ADDRESS SIZE = 8
 {
 '192.168.0.2' '192.168.0.3' '192.168.0.4'
 '192.168.0.5' '192.168.0.6' '192.168.0.7'
 '192.168.0.8' '192.168.0.9'
 }

 GROUP_ID = 177 SIZE = 2 { 'LEONID' 'SA' }
}
```

In this example, the groups represent different data types and `''` represents no condition.

## LIKE and NOT LIKE operator for groups

In the SR language used for advanced session-level policies, groups support the LIKE and NOT LIKE operators to search for wildcard values.

Example:

```
SR_POLICIES
{
 IF (CLIENT_IP NOT LIKE ('192.168.0.2',176) DB_USER = 'SCOTT') { VERDICT_DETACH }

 IF (CLIENT_IP != '192.168.0.3' DB_USER LIKE ('',177) { VERDICT_TERMINATE }

 GROUP_ID = 176 TYPE = IP_ADDRESS SIZE = 2
 {
 '192.168.%' '192.168.%'
 }

 GROUP_ID = 177 SIZE = 2 { 'LEON%' 'SA%' }
}
```

CIDR notation is supported for LIKE and NOT LIKE groups.

Examples:

```
192.168.1% Matches any IP starting with 192.168.1
2002:0920:C000:3146% Matches any IP starting with 2002:0920:C000:3146
192.168.128.1/17 11111111 11111111 10000000 00000000
 Allows 32K-2 (hosts) in the subnet(15 bits for the hosts)
 Similar to subnet mask of 255.255.128.0
2002:0920:C000:3146::0/61 11111111 11111111 11111111 11111111 11111111 11111111
 11111000 00000000 00000000 00000000 00000000 00000000
 00000000 00000000
 Allows 2^67 hosts on subnet 2002:0920:C000:3146::0/61
```

Note: For session-level policies created using the policy builder, use the following keywords to have a UI group considered as LIKE or NOT LIKE by default:

- `&#like:yes`
- `&#like:no`

## Grammar

Overall syntax and grammar used for creating advanced session-level policies.

Write advanced session-level policies using the basic format:

```
SR_POLICIES {
```

```

[TUPLES _ GROUP1, ... TUPLES _ GROUPn]

#RULE 1
IF (<conditions>)
{
 ACTION1

 ACTIONn
}

.....
#RULE m
IF (<conditions>)
{
 ACTION1

 ACTIONm
}

[GROUP1, GROUPk]

```

The complete advanced session-level policies scripting language (SR language) is expressed as:

- Mandatory fields: <...>
- Optional fields: [...]
- Allowed values separated by: |
- Rules, conditions, actions, tuples, and groups may contain one or more values.

To view the scripting language grammar, take the following steps:

1. Browse to the Guardium Security Policies > Create New Policy page.
2. Click Advanced session level policy.
3. Enter a new name for the policy and then click Rules.
4. From the top of the scripting worksheet, click Show Grammar.

## Unsupported databases for session-level policies

Databases and protocols that do not support session-level policies:

- CIFS
- Data Sets on z/OS
- Db2 on z/OS
- FTP
- IBM System i
- IMS

## Criteria

Criteria supported by session-level policies and advanced session-level policies include:

- Analyzed client IP address (ANALYZED\_CLIENT\_IP)  
Use this option when sessions are decrypted and the client IP address is not available.  
Restriction: Criteria ANALYZED\_CLIENT\_IP is the result of correlation encrypted and not encrypted sessions. This criteria is not always available.
- Analyzed client net mask (ANALYZED\_CLIENT\_NET\_MASK) (only supports = operator)  
Analyzed client net masks are possible additions to the IP address criteria. They represent the criterion IP address as a range of values.
- Application user (APP\_USER)
- Authentication type (AUTH\_TYPE)  
Use to differentiate by authentication methods. Allowed values:
  - WINDOWS
  - DATABASE
  - KERBEROS
  - ACTIVE\_DIRECTORY
  - NO\_AUTH
  - PLAIN
  - HTTP\_BASIC
  - BEARER
  - FEDERATION
  - GSSAPI
  - SCRAMSHA1
  - SCRAMSHA256
  - OS
  - SAML
  - LDAP
  - COOKIE
- Client host name (CLIENT\_HOST\_NAME)
- Client IP address (CLIENT\_IP)
- Client net mask (CLIENT\_NET\_MASK) (only supports = and != operators)

Client net mask is only available when using the client IP address parameter.

- Client operating system (CLIENT\_OS\_NAME)
- Command (COMMAND)

Search from the beginning of the SQL and do not use parser output. For example, with the statement `select sysdate from dual`, select will be recognized as the command.

When session-level policies use SQL criteria like command, object, or field, Guardium invokes the parser for these items before processing session-level criteria. If SQL criteria are not present in the policy, Guardium processes session-level criteria first and invokes the parser afterward.

- Client time zone (CTIMEZONE)

Use to limit the rule to a specific time zone of the client.

- Database name (DB\_NAME)

- Database protocol (DB\_PROTOCOL)

Use to differentiate databases by type and by the protocol version a database is using.

- Database type (DB\_TYPE)

- Database user (DB\_USER)

- Error (ERROR)
  - LOGIN\_FAILED

Use to search for specific database errors. Can be used to check for LOGIN\_FAILED.

- REQUEST\_ERROR

Use REQUEST\_ERROR in Tuples. It is not recommended to use REQUEST\_ERROR in Groups.

Note:

- Error criteria will be set to true for any error except LOGIN\_FAILED.

- Session level policy's ERROR criteria REQUEST\_ERROR is equivalent to Data Security Policy's Exception type criteria SQL\_ERROR.

- Field (FIELD)

When session-level policies use SQL criteria like command, object, or field, Guardium invokes the parser for these items before processing session-level criteria. If SQL criteria are not present in the policy, Guardium processes session-level criteria first and invokes the parser afterward.

- Incident (INCIDENT) (only supports = and != operators)

This detects problems related to protocol-level security. Allowed values:

- CREDENTIAL\_STUFFING

- PLAIN\_PASSWORD

Check if password is sent in plain text.

- WEAK\_PASSWORD

Check if password uses weak encryption.

- Label (LABEL) (supports = and != operators, and can contain tokens)

Use with LABEL actions to trigger actions based on a text string (the label). For more information, see [Label action and criteria](#).

- Literal (LITERAL) (supports =, !=, IN GROUP and NOT IN GROUP operators)

Use LITERAL to look for a specific value, or group of values, in a SQL statement.

- Network protocol (NET\_PROTOCOL)

The Policy Builder for Data provides a menu of valid network protocol values as well as supporting user-entered text values.

- Object (OBJECT)

When session-level policies use SQL criteria like command, object, or field, Guardium invokes the parser for these items before processing session-level criteria. If SQL criteria are not present in the policy, Guardium processes session-level criteria first and invokes the parser afterward.

- Operating system user (OS\_USER)

- Sender IP address (SENDER\_IP)

- Sender net mask (SENDER\_NET\_MASK) (only supports = and != operators)

Sender net mask is only available when using the sender IP address parameter.

- Server description (SERVER\_DESC)

Use for optional description of the database server. For example, from Guardium® Data Protection version 12.1 and later Server Description displays the cluster name of the Cloudera Data Platform.

- Server host name (SERVER\_HOST\_NAME)

- Server IP address (SERVER\_IP)

- Server net mask (SERVER\_NET\_MASK) (only supports = and != operators)

Server net mask is only available when using the server IP address parameter.

- Server operating system (SERVER\_OS\_NAME)

- Server port (SERVER\_PORT)

Use server port to differentiate multiple instances of the same database type on a single host.

- Service name (SERVICE\_NAME)

- Session (SESSION) (only supports = and != operators)

Allowed values:

- ADMIN

Check for administrator privileges. Supported for Oracle, PostgreSQL, Vertica, GreenPlum, Aster, and DB2 (DAS).

- ENCRYPTED

- FAILOVER

- FLAT\_LOG

- GET\_USERNAME\_PROBLEM

Applies when the Oracle Analyzer has identified a database user name retrieval issue.

- HIGH\_TRUST  
Apply actions to all sessions marked with HIGH TRUST\_LEVEL(GDM\_SESSION).
- LOCAL
- LOGGED
- LOGIN\_MISSED
- LOGIN\_RESTORED
- LOW\_TRUST  
Apply actions to all sessions marked with LOW TRUST\_LEVEL(GDM\_SESSION).
- MID\_STREAM
- NOT\_SUPPORTED\_PLATFORM
- PE\_ANOMALY  
Create rules when there is an exception identified by the probability engine.
- SENSITIVE  
Identify if session matches an extrusion pattern.
- SNIF\_LOGIN\_NOT\_COMPLETE
- STAP\_LOGIN\_NOT\_COMPLETE  
For UNIX S-TAP only: This criterion is supported for Linux-UNIX S-TAP only.  
A flag that indicates that priority packets were dropped within the first *N* packets of the session, where *N* is configured by the priority\_count parameter in the S-TAP guard tap.ini file.  
To track losses by S-TAPs or K-TAPs in reports, the transmit\_session\_losses\_metadata guard\_tap.ini parameter must be enabled (set to 1).
- For more information, see the [transmit\\_session\\_losses\\_metadata](#) and [priority\\_count](#) guard\_tap.ini parameters.
- STAP\_PACKETS\_DROPPED  
For UNIX S-TAP only: This criterion is supported for Linux-UNIX S-TAP only.  
A flag that indicates that packets were dropped within a session on the S-TAP side.
- TAP\_DECRYPTED
- U\_STAP
- W\_STAP
- SERVER\_DATA  
Supports patterns to search in server responses. Criteria can contain configuration parameters in the form of a set of bits, a search pattern in the form of a string (with wildcards), or a regular expression.  
Restriction:
  - Cannot be used with groups and tuples.
  - Only supports = operator.
  - This criterion can be configured to send data values to the logger.
  - For performance reasons, this criterion is checked last after all other criteria in the rule.
  - If built-in configuration options are set, then they have precedence over parameters defined in action CONFIGURE.

Syntax:

```
SERVER_DATA [$(configuration)$]<string_pattern|guardium_regex>
```

Where *configuration* is one of the following. Except where noted, the default is no.

- *count* - For regular expressions only. Data values are not provisioned. Counts only the number of matches.
- *values* - For regular expressions only. The number of matches is counted, and the data values are extracted.
- *sensitive* - Sets the rule session parameter as SENSITIVE, so that subsequent SESSION criteria can trigger specific actions related to SENSITIVE sessions.
- *masked* - For regular expressions only. Masks data values. (The data is masked with the "\*" character, leaving the last 4 characters unchanged).
- *luhn* - For regular expressions only. Applies a LUHN verification to extracted data. Used by default for credit card patterns. For other cases default is no.
- *greedy* - Sets the SERVER\_DATA criteria to verify all server response packets from the point when the first pattern was found, even if COMMAND or STATEMENT criteria do not match. When set to greedy, COMMAND and STATEMENT criteria of the rule are not verified.
- *lazy* - Disables the rule with a SERVER\_DATA criterion for the session where first 20 packets (priority packets) were checked.

The Policy Builder for Data provides controls for defining the server data configuration options.

In addition, <guardium\_regex> is one of the patterns described in [Guardium regex patterns](#).

- Session start time range (SESSION\_START) (only supports = and != operators)

This executes rules within a specific time range, for example to avoid logging and processing data from known periods of database optimization or back-up. For more information and detailed examples, see [Scheduling with SESSION\\_START examples](#).

- Source application (SOURCE\_PROGRAM)
- Statement (STATEMENT)

Use with wildcards to search the SQL statement.

Statement can be specified in the following format:

```
[Length] [Pattern] Length := $(integer[-integer])$
Pattern := <string>|<string with wildcards>|<guardium_regex>]
```

Where <guardium\_regex> is one of the patterns described in [Guardium regex patterns](#).

The Policy Builder for Data provides controls for defining the statement criteria based on maximum length, minimum length, length unit, and whether to check for bind variables.

Use the STATEMENT criterion with the SERVER.

Note: Session level policy's STATEMENT criteria is equivalent to the Data security policy's PATTERN criteria.

- Tuple (TUPLES)

Note:

- Check for empty criteria using either != '%' or = 'guardium://empty'.

- Hex values can be matched using \hd<xx> in criteria, patterns, group members, or tuple elements. For example: \hdf~~f~~OPERO matches <0xff>OPERO
- Identify binary non-ASCII symbols using the following: DB\_USER != 'GUARDIUM://LATIN'
- 

## Guardium regex patterns

---

Some criteria support <guardium\_regex>, which indicates a special regular expression that can include one of the following patterns:

- GUARDIUM://CREDIT\_CARD/MASTERCARD
- GUARDIUM://CREDIT\_CARD/VISA
- GUARDIUM://CREDIT\_CARD/AMEX
- GUARDIUM://CREDIT\_CARD/DINERS
- GUARDIUM://CREDIT\_CARD/DISCOVER
- GUARDIUM://CREDIT\_CARD/JCB
- GUARDIUM://CREDIT\_CARD/UNIONPAY
- GUARDIUM://CREDIT\_CARD/[MASTERCARD][|VISA][|AMEX][|DINERS][|DISCOVER][|JCB][|UNIONPAY]
- GUARDIUM://CREDIT\_CARD – Combines all 7 types of credit cards.
- GUARDIUM://PCI\_TRACK\_DATA

---

## Tuples

If several groups represent a union of parameters, create a tuple group to represent an intersection of parameters. Only one tuple group is allowed per rule.

Supported **TYPE** options:

- Analyzed client IP address (ANALYZED\_CLIENT\_IP)
- Application user (APP\_USER\_NAME)
- Authentication Type (AUTH\_TYPE)
- Client host name (CLIENT\_HOST\_NAME)
- Client IP address (CLIENT\_IP)
- Client operating system (CLIENT\_OS\_NAME)
- Command (COMMAND)
- C Time Zone (CTIMEZONE)
- Database name (DB\_NAME)
- Database protocol (DB\_PROTOCOL)
- Database type (DB\_TYPE)
- Database (DB\_USER)
- Error (ERROR)
- 12.1 and later Field (FEILD)
- Incident (INCIDENT)
- Network protocol (NET\_PROTOCOL)
- 12.1 and later Object (OBJECT)
- Operating system user (OS\_USER)
- 12.1 and later Literal (LITERAL)
- Sender IP address (SENDER\_IP)
- Server description (SERVER\_DESC)
- Server host name (SERVER\_HOST\_NAME)
- Server IP (SERVER\_IP)
- Server operating system (SERVER\_OS\_NAME)
- Server port (SERVER\_PORT)
- Service name (SERVICE\_NAME)
- Session (SESSION)
- Source application (SOURCE\_PROGRAM)
- Statement (STATEMENT)

Advance session-level policy examples

Example 1

```
TUPLES_GROUP_ID = 1 TYPE = (DB_USER OS_USER) SIZE = 5
{
 'sys%+oracle%' 'qa+q_a'
 '%scott+admin' 'guardium+guardium_%'
 '%system+admin'
}
```

This is an example of a 2-tuple group with five members.

Example 2

```
IF (SERVER_PORT = 1521 TUPLES = ('',1))
{
 TRANSFORM_DB_USER WHERE SOURCE = OS_USER OUTPUT_FORMAT = 'OPS$(.*)'
```

This is an example with tuples represented as parameters where the rule refers to **tuples\_group\_id = 1**. The **TRANSFORM\_DB\_USER** action takes the **OUTPUT\_FORMAT** and writes it to the **DB\_USER** field, where **OUTPUT\_FORMAT = 'OPS\$(.\*)'** means **OPS\$** plus all data from the field **OS\_USER**. **OUTPUT\_FORMAT** is a string, and it may include plain text, a regular expression result group, or the entire source string.

Example 3

```

SR_POLICIES
{
 TUPLES_GROUP_ID = 1 TYPE = (DB_USER OS_USER) SIZE = 6
 {
 '%sys+oracle%' 'qa+qa' 'sc??t+syb%'
 'sc??t+oracle%' 'system+admin' '%sc%+spo%'
 }
 TUPLES_GROUP_ID = 2 TYPE = (DB_USER OS_USER) SIZE = 4
 {
 '%sys+oracle%' 'qa+qa'
 '%sc%+spo%' 'OPS%+spo%'
 }

 IF (DB_USER != ('',1) { VERDICT_ATTACH }

 IF (SERVER_PORT = 1521 TUPLES = ('',1))
 {
 TRANSFORM_DB_USER SOURCE = OS_USER OUTPUT_FORMAT = 'OPS(.*)'
 }

 IF (TUPLES = ('',2))
 {
 TRANSFORM_CLIENT_HOST_NAME SEARCH_PREFIX = 'ENCORE' OUTPUT_FORMAT = 'PEREL'
 }

 GROUP_ID = 1 SIZE = 5 { 'root' 'sys' 'sa' 'admin' 'system' }
}

```

This is an example of tuples and groups used in the same policy. There can be multiple tuple groups in the same policy, but one rule can use only one tuple group. Create additional rules if you need to use additional tuple groups.

## Actions

Define audit, alerting, parsing and other actions to take when session-level policy rules are matched.

- [Audit and ignore session actions](#)  
Selective audit actions are triggered in analyzers before the parser/logger starts to receive session requests. Selective audit can save sniffer resources by reducing the load on relatively slower modules that limit sniffer performance.
- [Mark session actions](#)  
Mark session (MARK\_SESSION) is used to set a trust-level score from session-level policies or to control the learning of the real-time trust evaluator.
- [Alert and Log actions](#)
- [Parse actions](#)
- [Configure actions](#)  
The configure action is used to adjust analyzer settings or activate session-level policy features.
- [Transform actions](#)
- [Exception actions](#)
- [Extrusion actions](#)  
Use the REDACT and GET\_SERVER\_DATA actions to manage sensitive data.

## Audit and ignore session actions

Selective audit actions are triggered in analyzers before the parser/logger starts to receive session requests. Selective audit can save sniffer resources by reducing the load on relatively slower modules that limit sniffer performance.

### Audit only

This action is only available for policies that use the Selective Audit Trail setting. Audit Only logs the construct that triggered the rule. For a Selective Audit Trail policy, no constructs are logged by default, so use this selection to indicate which constructs you want to log. For example, for the Application Events API, if you want to log database usernames for reporting, use this action (otherwise, in this example, the username is blank).

### Discard session (DISCARD\_SESSION)

Discard session filters out the entire session. It sends a request to the S-TAP to ignore the session and not forward network traffic to the collector, for example encrypted data. Discard session supports search parameters and works with all supported traffic.

The following examples compare ignore session to discard session:

```

SR_POLICIES
{
 IF (DB_USER = 'SQLUSER1' SOURCE_PROGRAM = 'Vault')
 {
 DISCARD_SESSION
 }
}

SR_POLICIES
{
 IF (DB_USER = 'SQLUSER1' SOURCE_PROGRAM = 'Vault')
 {
 IGNORE_SESSION
 }
}

```

```
 }
```

During the login handshake, the S-TAP sends the initial DB\_USER and SOURCE\_PROGRAM values. Later, another packet might have the correct values for DB\_USER and SOURCE\_PROGRAM. The rule conditions for ignore session are checked earlier than the conditions for discard session, meaning that the discard session action is triggered later than the ignore session action.

## Ignore session (IGNORE\_SESSION)

Ignore session filters out the entire session. It sends a request to the S-TAP to ignore the session and not forward network traffic to the collector, for example encrypted data. Filtered sessions are not created, processed, or logged. Use ignore session with criteria that are known from the start of the session, for example database type, client IP address, or server IP address.

The following example filters out Hadoop traffic.

```
SR_POLICIES
{
 IF (DB_TYPE = 'HADOOP')
 {
 IGNORE_SESSION
 }
}
```

The following example uses (\*) to unconditionally ignore any sessions that are not logged after the first 50 packets arrive at the collector.

```
SR_POLICIES
{
 IF (*)
 {
 IGNORE_SESSION PACKETS_LIMIT = 50
 }
}
```

## Ignore request (IGNORE\_REQUEST)

Ignore requests that match search parameters.

This example ignores any SELECT statement that contains the pattern WARNING.

```
IGNORE_REQUEST WHERE REQ_TYPE = SQL SEARCH_PREFIX = 'SELECT' SEARCH_PATTERN = 'WARNING'
```

Note: For an Oracle data source, if you specify an IGNORE\_REQUEST action for a DBMS\_SESSION statement that updates some session parameters after parsing, then those session fields might not be set correctly for subsequent requests.

## Select session (SELECT\_SESSION)

Select session is the opposite of the ignore session action. It allows easy filtering and does not send a request to the S-TAP.

This example allows all sessions where the DB\_TYPE is not Hadoop. If the session is Hadoop, it is filtered by the sniffer.

```
IF (DB_TYPE != 'HADOOP')
{
 SELECT_SESSION
}
```

This example allows the collector to work only on the specified group of IPV6 S-TAPs.

```
IF (SENDER_IP = 'ad:f0:e1::1' SENDER_NET_MASK = 'ad:f0:e1::0')
{
 SELECT_SESSION
}
```

## Soft discard (SOFT\_DISCARD)

Soft discard is the same as discard session but does not send a command to the S-TAP and all processing is done on the collector. This provides something like a revocable discard that is available on a per-session basis. Soft discard is good for short sessions.

## Stop soft discard (STOP\_SOFT\_DISCARD)

Used for revoking the soft discard action, stop soft discard can revoke soft discard for individual sessions based on search parameters.

## Log access only (LOG\_ACCESS\_ONLY)

Log access forwards only the first required number of packets to the logger. No command is sent to the S-TAP. Log access allows only the following to pass to the logger: ACCESS\_INFO, FIRST\_REQUEST, LOGIN\_FAILED, ERRORS, TYPE\_UPDATE, TYPE\_LOGOUT, and TYPE\_LOGOUT\_TIMEOUT.

## Stop log access only (STOP\_LOG\_ACCESS\_ONLY)

Used for revoking the log access only action, stop log access can revoke log access only for individual session based on search parameters.

## Mark session actions

Mark session (MARK\_SESSION) is used to set a trust-level score from session-level policies or to control the learning of the real-time trust evaluator.

The mark session (MARK\_SESSION) action requires the as (AS) parameter. The as (AS) parameter supports the following values:

- Skip ML training phase (SKIP\_ML\_TRAINING\_PHASE)
- Skip ML evaluation (SKIP\_ML\_EVALUATION)
  - With (WITH)
- ML trusted (ML\_TRUSTED)
  - With (WITH)
  - Exception message (EXC\_MSG)
  - Track (TRACK)
    - True (TRUE)
    - False (FALSE)
  - Distinct (DISTINCT)
  - Label (LABEL)
- Set trust (SET\_TRUST)
  - With (WITH)
  - Exception message (EXC\_MSG)
  - Track (TRACK)
    - True (TRUE)
    - False (FALSE)
  - Distinct (DISTINCT)
  - Label (LABEL)

---

## Alert and Log actions

### Alert actions

---

Alert actions are only available through the policy builder for data UI for session-level policies and are not supported for advanced session-level policies. The following alert actions are available:

- Alert daily
- Alert once per session
- Alert only
- Alert per match
- Alert per time granularity

Alert actions allow an *exception message* that is added as part of the last error description in the alert message. Some alert actions also support the [distinct \(DISTINCT\) parameter](#).

Note: Alerting actions are not available for advanced session-level policies created using the SR language.

### Log actions

---

- 12.1 and later Audit only
- Log access only
- Log exception
- Log full details
- 12.1 and later Log full details with replaced values
- 12.1 and later Log masked details
- 12.1 and later Log Extrusion Counter
- 12.1 and later Log Masked Extrusion Counter
- 12.1 and later Log only

---

## Parse actions

The following parse actions are available:

- No parse (NO\_PARSE)
- Quick parse (QUICK\_PARSE)
- Quick parse no fields (QUICK\_PARSE\_NO\_FIELDS)

Parsing granularity is per-request.

---

## Configure actions

The configure action is used to adjust analyzer settings or activate session-level policy features.

The configure (CONFIGURE) parameter accepts the following options:

- ANALYZER\_PARSER:<ON|OFF>  
Disable to require processing session-level criteria before invoking the parser, regardless of whether SQL criteria like command, object, or field are used in the policy.

- CHARSET:guardium://char\_set?<hint|force>=<int>  
Use alternative character set.
- CREDENTIAL\_STUFFING:<ON>|[PMAX=<float>]|,[CONFIDENCE=<float>]  
Start credential stuffing attack detector.
- 12.1 and later DISABLE\_CACHE:ALL|[HOSTNAME][,SERVICENAME][,OSNAME]  
Disables caching of Host names, Service names, OS names separately or all together.
- IFX\_IGNORE:OFF  
Tell Informix analyzer to stop ignoring sessions.
- IGNORED\_FLAG:<ON|OFF>  
Enable to log sessions otherwise ignored with the following actions: DISCARD SESSION, SOFT DISCARD SESSION, LOG ACCESS ONLY, STOP LOG ACCESS ONLY, STOP SOFT DISCARD. This setting is not required with the LOG ACCESS ONLY action. The default value is OFF.
- 12.1 and later LARGE\_RESULTSET:<ON|OFF>  
Removes size limits for database responses. The default value is ON.
- LOG\_PARSER\_ERRORS:<ON|OFF>  
Enable or disable logging parser errors. The default value is ON.
- LOG\_CONSTRUCT\_ERRORS:<ON|OFF>  
Enable or disable logging construct errors. The default value is OFF.
- MARK\_BATCH:<ON|OFF>  
Enable to mark SQL execution as part of a batch. The default value is OFF.
- ORA\_BIND\_TYPE:<SELECT|INSERT|UPDATE|DELETE>  
Oracle bind variable type.
- ORA\_CHECKSUM:<MD5|SHA1|SHA256|SHA384|SHA512|int>  
Type of Oracle hash used in Oracle data integrity.
- ORA\_SESSION\_INFO:<session\_info\_string>  
Oracle session platforms.
- ORA\_TOKEN\_OFFSET:<TNS314|TNS315>  
Token format for calculating Oracle statement size.
- QUERY\_REWRITE:<ON|OFF>  
Enable to attach or detach based on session-level criteria.
- RAW\_STATEMENT\_MAP\_SIZE:<integer>  
Change the number of raw statements stored in the analyzer. The default value is 1024 raw statements per session.
- SELECTIVE\_AUDIT:ON  
Selective audit actions are triggered in analyzers before the parser/logger starts to receive session requests.
- SERVER\_DATA:[OFF]|[MAX\_HITS=<integer>]|[CONFIDENCE=<integer>]|[EXFILTRATION=<integer>]  
Used in combination with other criteria, the SERVER\_DATA criteria allows limiting the scope of extrusion rules to improve performance.
  - OFF - Turn off checking the criteria according to its CONFIGURE abilities.
  - MAX\_HITS - Applies to regular expressions only and refers to the maximum number of pattern matches in a packet. The default value is 1, meaning SERVER\_DATA is used as the usual criteria for finding at least one match.
  - CONFIDENCE - Applies to regular expressions only using the COUNT or VALUE flags, it refers to the number of checks before deciding that matches are not false positives. The default value is 1.
  - EXFILTRATION - Applies to regular expressions only and limits the number of hits per request. If the session is SENSITIVE, exceeding this limit may indicate exfiltration of sensitive data. In this case, SENSITIVE\_DATA\_EXFILTRATION is set.
- SESSION\_TRUST:<OFF>|[LOW=<float>]|,[HIGH=<float>]  
Exclude sessions from session trust evaluation or change LOW/HIGH trust limits.
- STRICT\_USERNAME:<replacement\_value>  
Where <replacement\_value> is any value that you choose. If Guardium finds a problem with the username, it is replaced with the specified value.
- TDS\_SWAP\_LIMIT:<number between 10,000 and 100,000>  
MS SQL analyzer related to records affected calculation.
- TYPE\_STATUS:<ON|OFF>  
Disable to prevent logging sessions with artificial activities.

## Transform actions

Available transform actions:

- TRANSFORM ANALYZED CLIENT IP (TRANSFORM\_ANALYZED\_CLIENT\_IP)
- TRANSFORM APP USER NAME (TRANSFORM\_APP\_USER)
- TRANSFORM CLIENT HOST NAME (TRANSFORM\_CLIENT\_HOST\_NAME)
- TRANSFORM CLIENT OS NAME (TRANSFORM\_CLIENT\_OS\_NAME)
- TRANSFORM DB NAME (TRANSFORM\_DB\_NAME)
- TRANSFORM DB USER (TRANSFORM\_DB\_USER)
- TRANSFORM OS USER (TRANSFORM\_OS\_USER)
- TRANSFORM SERVER DESCRIPTION (TRANSFORM\_SERVER\_DESC)

- TRANSFORM SERVER HOST NAME (TRANSFORM\_SERVER\_HOST\_NAME)
- TRANSFORM SERVER OS NAME (TRANSFORM\_SERVER\_OS\_NAME)
- TRANSFORM SERVICE NAME (TRANSFORM\_SERVICE\_NAME)
- TRANSFORM SOURCE PROGRAM NAME (TRANSFORM\_SOURCE\_PROGRAM)
- TRANSFORM STATEMENT (TRANSFORM\_STATEMENT)

## Transform action examples in the UI

---

For an example of how to use the TRANSFORM ANALYZED CLIENT IP action, see [Hostname caching example](#).

For an example of how to use the TRANSFORM DB NAME action, see [Add DB name on failed login example](#).

For some examples of how to use the TRANSFORM STATEMENT action, see [Query masking examples](#).

For more information about creating session level policies in the UI, see [Understanding the UI examples](#).

## Transform action examples using the advanced session-level policy language

---

Example:

```
TRANSFORM_SERVER_DESC SEARCH_PREFIX = 'SERVER_DESCRIPTION:guardium://empty' OUTPUT_FORMAT = 'IBM VM'
```

This shows the use of tokens in a transform action such that if the SERVER\_DESCRIPTION field is empty for the session it is transformed to IBM VM.

Example:

```
SEARCH_PREFIX = 'DB_USER:SCOTT'
SEARCH_PATTERN = 'OS_USER:ORACLE19'
MATCH_PATTERN = 'SOURCE_PROGRAM:/(\w+)/(.*))'
```

These show the ability to use independent targets.

Example of using "not found" (NOT), which is available in SEARCH\_PREFIX, SEARCH\_PATTERN, and MATCH\_PATTERN:

```
SEARCH_PREFIX = '(NOT):STATEMENT:grant' - means any not "GRANT ..." statement.
SEARCH_PREFIX = '(NOT):OS_USER:? - empty OS user.'
```

These show how to use SEARCH\_PREFIX to match any statement other than grant and an empty OS user, respectively.

Example:

```
TRANSFORM_DB_USER SEARCH_PREFIX = '(NOT):(DB_USER)' SOURCE = OS_USER OUTPUT_FORMAT = '$(SOURCE_PROGRAM)$\(.*)'
Initial GDM_ACCESS record:
DB_USER = *scott*. | OS_USER = oracle19 | SOURCE_PROGRAM = sqlplus

Transform result in GDM_ACCESS table:
DB_USER = sqlplus\oracle19 | OS_USER = oracle19 | SOURCE_PROGRAM = sqlplus
```

### Case 1:

#

Special handling for TRANSFORM actions:

According to EX. 1 CLIENT\_HOST\_NAME should be transformed into IP address and copied to ANALYZED\_CLIENT\_IP field, but in addition it is possible to check and do it only if analyzed client IP is empty:

```
TRANSFORM_ANALYZED_CLIENT_IP SEARCH_PREFIX = '(NOT):ANALYZED_CLIENT_IP:?' SOURCE = CLEINT_HOST_NAME OUTPUT_FORMAT = '(.*)'
```

### Case 2:

```
TRANSFORM_DB_USER WHERE OUTPUT_FORMAT = '<some string>' # copies <some string> into DB_USER, if DB_USER is empty (not copies if DB_USER is not empty)
```

### Case 3:

```
TRANSFORM_DB_USER WHERE SEARCH_PREFIX = '?' OUTPUT_FORMAT = '<some string>' # copies <some string> into DB_USER, if DB_USER is not empty (not copies if DB_USER is empty)'
```

Now it is possible to transform to some value to empty. For that in any transform action it is possible to put SEARCH\_PREFIX = '?' and OUTPUT\_FORMAT as 'guardium://empty'

## Specific behaviors for search parameters with transform actions

---

Transform actions using certain search parameters may have specific behavior, as illustrated by the following examples.

Example:

```
TRANSFORM_DB_USER WHERE SOURCE = OS_USER OUTPUT_FORMAT = '(.*)'
```

This always copies OS\_USER into DB\_USER, regardless of whether or not DB\_USER is empty.

Example:

```
TRANSFORM_ANALYZED_CLIENT_IP SEARCH_PREFIX = '(NOT):ANALYZED_CLIENT_IP:?' SOURCE = CLEINT_HOST_NAME OUTPUT_FORMAT = '(.*)'
```

This transforms CLIENT\_HOST\_NAME into an IP address and copies it to ANALYZED\_CLIENT\_IP only if ANALYZED\_CLIENT\_IP is empty.

Example:

```
TRANSFORM_DB_USER WHERE OUTPUT_FORMAT = '<some string>'
```

This copies <some string> into DB\_USER only if DB\_USER is empty. It will not copy the value if DB\_USER is not empty.  
Example:

```
TRANSFORM_DB_USER WHERE SEARCH_PREFIX = '?' OUTPUT_FORMAT = '<some string>'
```

This copies <some string> into DB\_USER only if DB\_USER is not empty. It will not copy the value if DB\_USER is empty.  
Example:

```
TRANSFORM_DB_USER WHERE SEARCH_PREFIX = '?' OUTPUT_FORMAT = 'guardium://empty'
```

This transforms DB\_USER to an empty value.

- [Transform parameters](#)

Transform actions support additional parameters not available with other actions.

---

## Transform parameters

Transform actions support additional parameters not available with other actions.

### Source (SOURCE)

Source is used as a filter to tell the action which value should be matched. Values include:

- ANALYZED CLIENT IP (ANALYZED\_CLIENT\_IP)
- APP USR NAME (APP\_USER\_NAME)
- CLIENT HOST NAME (CLIENT\_HOST\_NAME)
- CLIENT OS NAME (CLIENT\_OS\_NAME)
- DB NAME (DB\_NAME)
- DB USER (DB\_USER)
- OS USER (OS\_USER)
- SERVER DESCRIPTION (SERVER\_DESC)
- SERVER HOST NAME (SERVER\_HOST\_NAME)
- SERVER IP (SERVER\_IP)
- SERVER OS NAME (SERVER\_OS\_NAME)
- SERVICE NAME (SERVICE\_NAME)
- SOURCE PROGRAM NAME (SOURCE\_PROGRAM)
- STATEMENT (STATEMENT)

The source parameter defines the content used for search parameters in transform actions.

Example:

```
TRANSFORM_DB_USER SEARCH_PREFIX = 'CHE' SOURCE = OS_USER OUTPUT_FORMAT = '(.*)'
```

This copies the value of OS\_USER to DB\_USER if OS\_USER begins with the string CHE.

### Mask (MASK)

Mask uses the regular expression defined by the match pattern parameter to search the source and replace (mask) all matched occurrences using the value defined by the output format parameter. Use the mask parameter with match pattern (MATCH\_PATTERN) and output format (OUTPUT\_FORMAT). For example

Example:

```
TRANSFORM_OS_USER SEARCH_PREFIX = '?' MATCH_PATTERN = '\d' MASK_OUTPUT_FORMAT = '0'
```

This matches all digits and replaces them with 0, such that if OS\_USER is ORACLE19 it becomes ORACLE00.

### Output format (OUTPUT\_FORMAT)

Output format defines the output for transform actions. When source (SOURCE) is specified, the output format can be (.) to replace the transformed value with the source value. When used with match pattern, custom strings and the contents of regular expression groups like \1 can be used. Specify **guardium://empty** for empty output.

### Related concepts

- [Search parameters](#)
- 

## Exception actions

Available exception actions:

- Throw exception (THROW\_EXCEPTION)
- Log exception (LOG)

### Throw exception (THROW\_EXCEPTION)

Throw exception accepts an exception type that defines what type of processing happens on the logger side. Exception message (EXC\_MSG) allows customization of the message. Available exception types:

- Analyzer alert
- Security incident
  - Adds the exception to the Security incidents report.
- Session exception

## Log exception (LOG)

Log exception is the same as throw exception but can be used to log an exception even when the login is not made.

## Extrusion actions

Use the REDACT and GET\_SERVER\_DATA actions to manage sensitive data.

Available extrusion actions:

- REDACT
- GET\_SERVER\_DATA

## REDACT

The REDACT action requires *log record affected* and *inspect return data* to be enabled for the inspection engine. It is executed on analyzer level of sniffer processing and can prevent execution of the first SQL statement without redaction being applied with the firewall mode activated.

Attention: The REDACT action alters raw packets. Using broad regular expressions can inadvertently modify internal data structures sent by the server, potentially causing session disruptions. To avoid these issues, be sure to use precise regular expressions that avoid false positives. In addition, if patterns are spread across two physical network packets or their fragments, REDACT operations might be skipped, because S-TAP does not assemble these packets.

For more information about using REDACT, including additional restrictions, see [Redact](#) in [Logging or ignoring rule actions](#).

Note:

- Write the part of the pattern that you want to mask in parentheses.
- 12.1 and later Along with the list of predefined replacement symbols, you can enter any custom symbol as a replacement symbol.

## GET\_SERVER\_DATA

The Runtime Sensitive Object Identification policy uses the GET\_SERVER\_DATA action to retrieve and process sensitive data. This action is available only for use with the Runtime Sensitive Object Identification policy.

## Action parameters

- [Label action and criteria](#)  
Use the Label (LABEL) action parameter to assign a label to the triggered action, which you can then use as a criterion for subsequent rules.
- [Distinct parameter](#)  
The distinct (DISTINCT) parameter is a flexible way to group different sessions at runtime.
- [Track option](#)  
The track option allows you to trace the execution action of session-level policies.
- [Search parameters](#)  
Search parameters define additional conditions and can be used with different actions.

## Label action and criteria

Use the Label (LABEL) action parameter to assign a label to the triggered action, which you can then use as a criterion for subsequent rules.

You can use both the LABEL action and LABEL criteria as follows:

Within a policy, let's say you define a LABEL action as

```
LABEL = (DB_USER)
```

If this action is triggered for some session request (such as **DB\_USER** = SCOTT), then SCOTT is added to internal dynamic group.

In addition, let's say that you create a rule within the policy that has the following criteria:

```
LABEL = (DB_USER)
```

If a request comes in from a database user, then the LABEL criteria is triggered. If the database user (the DB\_USER) is, for example, SA, then that DB\_USER is not found in dynamic group, the criteria LABEL is validated to false, and the rule actions are not triggered. However, if the request comes the database user SCOTT, then SCOTT is found in the dynamic group, and the LABEL criteria is validate to true, which triggers the rule actions.

The LABEL parameter is available for the following actions:

- ALERT
- IGNORE\_REQUEST
- LOG
- MARK\_SESSION
- THROW\_EXCEPTION
- VERDICT\_TERMINATE

## Distinct parameter

The distinct (DISTINCT) parameter is a flexible way to group different sessions at runtime.

The distinct parameter is used with the following actions:

- ALERT\_ONCE\_PER\_SESSION
- ALERT\_ONLY
- ALERT\_PER\_MATCH
- DISCARD\_SESSION
- IGNORE\_REQUEST
- LOG
- MARK\_SESSION
- THROW\_EXCEPTION
- VERDICT\_TERMINATE

Syntax:

```
Syntax:
<distinct> ::= [MIN_COUNT=<number><space>] [PERIOD=<number><space>] [MAX_COUNT=<number><space>] [RESET_INTERVAL=<number>[:<number>]<space>] [composite key]$
<composite key> ::= [<key>|<FUNC|key|[condition key]>]
<FUNC> ::= <SUM>
<key> ::= [<token>...<token|>]
<condition key> ::= [<token>...<token|>]
<token> ::= $(<session parameter>)$
<session parameter> ::= <DB_USER|CLIENT_IP|CLIENT_HOST_NAME|SERVER_IP|SERVER_HOST_NAME|
 OS_USER|DB_NAME|DB_TYPE|SOURCE_PROGRAM|SERVICE_NAME|NET_PROTOCOL|
 ANALYZED_CLIENT_IP|COMMAND|ERROR|SENDER_IP>
```

```
MIN_COUNT value is any >0 and <= 65535.
PERIOD value is the number >0 and <=65535
MAX_COUNT value is any >0 and <= 65535.
RESET_INTERVAL measured in minutes.
CON_MIN_COUNT value is any >0.
CON_MAX_COUNT value is any >0.
```

Examples:

| CLIENT_IP         | DB_USER | SOURCE_PROGRAM | COUNT |
|-------------------|---------|----------------|-------|
| 9.70.2.3.1        | SCOTT   | SQLPLUS        |       |
| 19.70.2.3.1       | SCOTT   | TOAD           |       |
| 19.70.2.3.1       | SCOTT   | JDBC           |       |
| 19.70.2.3.1       | SYS     | JDBC           |       |
| 19.70.2.3.1       | ALICE   | TOAD           |       |
| 19.70.2.3.2       | SCOTT   | SQLPLUS        |       |
| 19.70.2.3.2       | BOB     | SQLPLUS        |       |
| 29.70.2.3.2       | BOB     | TOAD           | 1     |
| <hr/>             |         |                |       |
| TOTAL CONNECTIONS |         |                | 9     |
| TOTAL PROGRAMS    |         |                | 3     |
| TOTAL USERS       |         |                | 5     |
| TOTAL CLIENTS     |         |                | 2     |

- More than 2 connections from different users of same CLIENT\_IP during 1 minute (Client - 9.70.2.3.1, 3 Users - SCOTT, SYS, ALICE):
 

```
MIN_COUNT=3 MAX_COUNT=3 RESET_INTERVAL=1 SUM|(DB_USER)|$(CLIENT_IP)$$
```
- More than 3 connections from different users during 1 minute (4 occurrences: SCOTT,SYS,ALICE,BOB):
 

```
MIN_COUNT=4 MAX_COUNT=4 RESET_INTERVAL=1 SUM|(DB_USER)|$
```
- More than 3 connections from same users during 1 minute (User SCOTT):
 

```
MIN_COUNT=4 MAX_COUNT=4 RESET_INTERVAL=1 $(DB_USER)$$
```
- More than 2 connections from same user of same CLIENT\_IP during 1 minute (Client - 9.70.2.3.1, User - SCOTT and Client - 9.70.2.3.2, User - BOB):
 

```
MIN_COUNT=3 MAX_COUNT=3 RESET_INTERVAL=1 (DB_USER)|$(CLIENT_IP)$$
```
- More than 1 connection from different users and source programs of same CLIENT\_IP during 1 minute (Client - 9.70.2.3.1, Client - 9.70.2.3.2):
 

```
MIN_COUNT=2 MAX_COUNT=2 RESET_INTERVAL=1 SUM|(DB_USER)|$(SOURCE_PROGRAM)$|$(CLIENT_IP)$$
```
- More than 1 connection from same user, same program of same CLIENT\_IP during 1 minute (Client - 9.70.2.3.2, User - BOB, PROGRAM - SQLPLUS):
 

```
MIN_COUNT=2 MAX_COUNT=2 RESET_INTERVAL=1 (DB_USER)|$(SOURCE_PROGRAM)$|$(CLIENT_IP)$$
```
- Too many db users connecting from same client ip per period of time (SESSION != 'TAP\_DECRYPTED'):
 

```
MIN_COUNT=10 MAX_COUNT=10 RESET_INTERVAL=5 SUM|(DB_USER)|$(CLIENT_IP)$$
```
- Find user with reused password (DB\_USER!=%''):
 

```
MIN_COUNT=2 SUM|(DB_USER)|$(PASSWORD)$$
```

```
9. Too many Login failures from same Program and different DB users per period of time (5 in 3 minutes).
MIN_COUNT=5 MAX_COUNT=5 RESET_INTERVAL=3 SUM|$(DB_USER)|$(SOURCE_PROGRAM) $$
```

## Track option

The track option allows you to trace the execution action of session-level policies.

The track option is available for the following actions:

- Ignore session (IGNORE\_SESSION)
- Discard session (DISCARD\_SESSION)
- Log access only (LOG\_ACCESS\_ONLY)
- Stop log access only (STOP\_LOG\_ACCESS\_ONLY)
- Soft discard session (SOFT\_DISCARD\_SESSION)
- Stop soft discard session (STOP\_SOFT\_DISCARD\_SESSION)
- Mark session (MARK\_SESSION) when as (AS) value is not ML TRUSTED (ML\_TRUSTED)
- S-Gate session terminate (S-GATE\_SESSION\_TERMINATE)

## Search parameters

Search parameters define additional conditions and can be used with different actions.

### Request type (REQ\_TYPE)

Request type acts as a filter for transform actions. In non-transform actions with search parameters, request type provides a hint for where to search.

Request types available for actions with search parameters:

- LOGIN FAILED (LOGIN\_FAILED)
- PREPARED STATEMENT (PREP\_STAT)
- RPC (RPC)
- SQL (SQL)
- SQL ERROR (SQL\_ERROR)
- SQL SUCCESS (SQL\_SUCCESS)

Request types available for actions with transform parameters:

- LOGIN FAILED (LOGIN\_FAILED)
- PREPARED STATEMENT (PREP\_STAT)
- RPC (RPC)
- SQL (SQL)
- SQL ERROR (SQL\_ERROR)

Note: In the SR language, write request types without quotation marks.

### Search prefix (SEARCH\_PREFIX)

Search prefix matches the defined pattern at the beginning of a value.

Use search prefix with or without request type for transform actions and for regular actions with search parameters. Request type acts as a filter for transform actions. In non-transform actions with search parameters, request type provides a hint for where to search.

| Rule criteria used          |     |     |     |     |
|-----------------------------|-----|-----|-----|-----|
| Request type defined        | Yes | No  | Yes | No  |
| Search prefix defined       | Yes | Yes | No  | No  |
| Actions taken               |     |     |     |     |
| Search with search prefix   | Yes | Yes | No  | No  |
| Search with request type    | No  | No  | Yes | No  |
| Search in DB User (DB_USER) | No  | No  | No  | Yes |

Example:

```
IGNORE_REQUEST REQ_TYPE = SQL SEARCH_PREFIX = 'GAT'
```

This matches SQL requests with the prefix GAT.

Example:

```
IGNORE_REQUEST REQ_TYPE = SQL_ERROR SEARCH_PREFIX = 'TNS-'
```

This matches SQL errors with the prefix TNS-.

### Search pattern (SEARCH\_PATTERN)

Search pattern matches the defined pattern in any part of the value.

Example:

```
IGNORE_REQUEST REQ_TYPE = SQL SEARCH_PREFIX = 'SELECT' SEARCH_PATTERN = 'FROM SCOTT.'
```

This matches SELECT SQL requests that contain the pattern FROM SCOTT.

## Match pattern (MATCH\_PATTERN)

---

Match pattern is similar to search pattern but uses regular expressions to match the defined pattern in any part of the value.

Example:

```
SELECT * FROM SCOTT.A WHERE SECRET = '1234'
MATCH_PATTERN = '^.*FROM (.*)\\.A\\.*$'
OUTPUT_FORMAT = '\1'
```

This takes the first regular expression element in parenthesis and writes it to the output format.

## Search offset (SEARCH\_OFFSET)

---

Search offset works with search pattern and match pattern to cut the source string where the matched pattern is found. This can improve matching with regular expressions.

Example:

```
SELECT LAST_NAME FROM SCOTT.EMPLOYEES
TRANSFORM STATEMENT SEARCH_PREFIX = 'SELECT' SEARCH_PATTERN = 'FROM SCOTT.' SEARCH_OFFSET MATCH_PATTERN = '^(.*)\\. (.*)$'
OUTPUT_FORMAT = '\1.\2'
```

This finds the string defined by search pattern while search offset cuts off everything before it allowing match pattern to work more efficiently.

## Checking criteria for actions in search parameters

---

The default is `DB_USER:guardium://empty`, meaning that SEARCH\_PREFIX matches if the value is empty. Other criteria can be checked:

- ANALYZED\_CLIENT\_IP
- APP\_USER\_NAME
- AUTH\_TYPE
- CLIENT\_HOST\_NAME
- CLIENT\_IP
- CLIENT\_OS\_NAME
- COMMAND
- CTIMEZONE
- DB\_NAME
- DB\_USER
- DESCRIPTION
- ERROR
- OS\_USER
- SERVER\_DESCRIPTION
- SERVER\_HOST\_NAME
- SERVER\_IP
- SERVER\_OS\_NAME
- SERVICE\_NAME
- SOURCE\_PROGRAM
- STATEMENT

Examples:

- Search prefix = `DB_USER:NO_AUTH`
- Search pattern = `STATEMENT:SELECT%`
- Match pattern = `ERROR:%13%`

## Session-level policy examples

---

To help you understand session-level policies, Guardium provides a number of examples with descriptions. The examples include both the Guardium UI and SR language methods.

### Understanding the UI examples

---

These examples might help you understand how to design and build session-level policies.

For the UI examples, each example describes the actions that you need to take on each ribbon to re-create the example, as follows:

1. For the *Ignoring sessions example* policy, start with creating and naming the policy, as described in [Creating session-level policies](#). Select Session level policy and provide a name.

## Create New Policy

Name and properties  
Provide a unique name and optional properties

Type: Session level policy

Name: Ignore sessions

Roles: No roles assigned.

Rules: Number of rules: 0

2. Click the Rules ribbon and then click the icon to open the Create New Rule window. For this policy, you need to provide only the name of the first rule.

### Create New Rule

Rule definition  
Specify rule name and type

Rule type: Session

Rule name: Rule 1

Category: Enter rule category

Classification: Enter rule classification

Severity: Information

Rule criteria: No parameters specified

Rule action: Number of actions: 0

3. Click the icon to open the Create New Rule window. From here, you can add session-level criteria.

Note: In the examples, the criteria are labeled as Session level criteria. For example, in [Ignoring sessions example](#), this example is shown as:

#### Session level criteria

- Client IP address = 10.10.10.10
- Server IP address = 20.20.20.20
- Source application = JAVA%

Add criteria as needed by clicking the near the last criterion.

Figure 1. Rule criteria UI example

### Create New Rule

Rule definition: Rule 1

Rule criteria: Conditions where rule action will be triggered

Session level criteria

|                    |   |             |
|--------------------|---|-------------|
| Client IP address  | = | 10.10.10.10 |
| Client net mask    | = | 0.0.0.0     |
| Server IP address  | = | 20.20.20.20 |
| Server net mask    | = | 0.0.0.0     |
| Source application | = | JAVA%       |

Rule action: Number of actions: 0

4. When you are done adding criteria, click the Rule action ribbon, and then click the to begin adding actions.

Note: In the examples, the rule actions are labeled as Rule action. The example documentation describes only the criteria that you need to change for a specific example.

Figure 2. Add new action UI example

Create New Rule

Rule definition: Rule 1

Rule criteria: 3 session parameters specified

Rule action

Add New Action

\* Rule action: IGNORE SESSION

Packets limit: 1

Track: True False

OK Cancel

5. When you are done, your new policy looks similar to the following policy,

Figure 3. Session level policy with rules and actions

The screenshot shows a 'Session level policy' configuration screen. At the top, there are tabs for 'Name and properties' (selected) and 'Ignore sessions policy'. Below is a 'Rules' section with a 'Define policy rules' tab selected. A toolbar includes icons for add, edit, delete, import, reinstall, and uninstall. A 'Filter' button is also present. The main area displays two rules:

| Order | Rule type | Rule name | Tags | Criteria                                                                                                      | Actions        | Continue to next rule | Installed |
|-------|-----------|-----------|------|---------------------------------------------------------------------------------------------------------------|----------------|-----------------------|-----------|
| 1     | Session   | Rule 1    |      | Server IP address = 20.20.20.20, Client IP address = 10.10.10.10, Source application = JAVA%, Severity = Info | IGNORE SESSION |                       |           |
| 2     | Session   | Rule 2    |      | Severity = Info                                                                                               | IGNORE SESSION |                       |           |

In addition, each example includes an advanced session-level policy that is written in the SR language.

## Mapping the SR language examples

In the SR language examples, you can map the parameters (that is, parameter = *variable*) directly to most UI examples. Take for example the following SR language snippet:

```
SR_POLICIES
{
 IF (CLIENT_IP = '10.10.10.10' SOURCE_PROGRAM = 'JAVA%' SERVER_IP = '20.20.20.20')
 {
 IGNORE_SESSION
 }
 IF (*)
 {
 IGNORE_SESSION PACKETS_LIMIT = 50
 }
}
```

- CLIENT\_IP criteria in the SR language maps to Client IP address in the UI
- SERVER\_IP maps to Server IP address.
- SOURCE\_PROGRAM maps to Source application.

In addition, the { `IGNORE_SESSION` } code in the SR language maps to the IGNORE SESSION rule action in the UI.

In the [Using session-level and advanced session-level policies](#), you can find the mappings between the SR language and UI elements.

In the guide, the UI name is generally on the left, and the SR language name is on the right. The SR language name is shown in parentheses. For example, looking at search parameters:

Request types available for actions with search parameters:

```
LOGIN FAILED (LOGIN_FAILED)
PREPARED STATEMENT (PREP_STAT)
RPC (RPC)
SQL (SQL)
SQL ERROR (SQL_ERROR)
SQL SUCCESS (SQL_SUCCESS)
```

LOGIN FAILED in the UI maps to LOGIN\_FAILED in the SR language, PREPARED STATEMENT in the UI maps to PREP\_STAT in the SR language.

- [Ignoring sessions example](#)  
The [Ignore sessions](#) policy shows two different methods of ignoring certain policies.
- [Log LOGIN FAILED sessions only example](#)  
The [Log LOGIN FAILED sessions only](#) policy contains a single rule that logs an error if a login fails. Other types of errors that the session encounters are ignored.
- [REQUEST\\_ERROR example](#)  
REQUEST\_ERROR in the session level policies are SQL errors.
- [Add DB name on failed login example](#)  
The [Add DB name on failed login](#) policy solves a problem where the database name is not available if the login fails (with a LOGIN\_FAILED message). If the DB\_NAME value is empty, the policy adds a database name.
- [Get correct service name \(MS SQL Server\) example](#)  
For MS SQL server, some sites use a placeholder name for the SERVICE\_NAME. This example shows how to replace the placeholder with the actual service name.
- [Ignoring exceptions example](#)  
The [Ignoring exceptions](#) policy shows two ways to ignore certain exceptions.
- [Firewall and latency issues examples](#)  
If your site uses the Guardium® database firewall, you can encounter latency issues when Guardium reconnects. These examples show how to use session-level policies to prevent unwanted traffic.
- [Sniffer overload issues examples](#)  
In some circumstances, the Guardium sniffer can be overloaded with unnecessary traffic. These three examples show how to prevent the traffic that can overload the sniffer, while still allowing other traffic through.
- [Query masking examples](#)  
Analyzer query masking can be useful when used with non-relational databases such as MongoDB or Cassandra, or protocol frameworks such as the Google protocol buffer or Apache Thrift. The following examples show how to mask unencrypted data in non-relational databases.
- [Correct IP address \(Oracle\) example](#)  
When the Oracle connection manager handles the connection to the database server, the connection manager can insert the wrong IP address and other information. The following example shows how to ensure that Guardium has the correct information from Oracle.
- [Show SQL schema names example](#)  
You can use a session-level policy to find and display an SQL schema name. This example shows how to move the schema name to the `GDM_CONSTRUCT_INSTANCE.APP_USER_NAME` table and column so that it is available for reports.
- [Server and S-TAP IP addresses example](#)  
For some Guardium implementations, one collector serves multiple S-TAPs. In some cases, customers want to have separate sets of session-level policies for each S-TAP. Normally they can use SERVER\_IP and SERVER\_NET\_MASK rule conditions. However, the server IP address can be different from STAP IP address. In these cases, use a session-level policy to associate the session-level policies by S-TAP.

- [User authentication \(Oracle\) example](#)  
If your site uses Oracle OS authentication, the DB\_USER cannot be captured in network traffic and therefore is not logged. For this session-level policy, if the DB\_USER is empty, the policy copies the ORACLE\_USER name to DB\_USER.
- [Redacting data example](#)  
The REDACT rule action is similar to redaction in extrusion rules. Use REDACT to replace a matched pattern in SQL statements that are sent from client to server and mask the matched values.
- [Hostname caching example](#)  
This example shows how to manage hostnames that are stored in a cache file, where the cache is updated hourly.
- [Ignore specified users example \(MongoDB\)](#)  
This example ignores all requests that belong to the MongoDB users NO\_AUTH and \_SYSTEM.
- [Scheduling with SESSION\\_START examples](#)  
Use SESSION\_START to define when the session-level rules are active. The following examples show how to use the Session start time range parameter.
- [Logging access activity for trusted sessions example](#)  
You can change LOG\_ACCESS\_ONLY functionality by using IGNORE\_REQUEST as shown in the following examples.
- [Creating a custom exception message example](#)  
Create a custom exception message with the SR language THROW\_EXCEPTION or by selecting the LOG EXCEPTION action in the UI for a local session-level policy.
- [Find name in SQL query example](#)  
Create a session-level policy that sends an alert when a name is found in an SQL query.
- [Detect local admin example](#)  
Use this policy to attach local admin sessions.
- [Strict username example \(Oracle\)](#)  
Monitoring network traffic is subject to network packet loss. Losses can occur for various reasons, such as overloading S-TAP buffers on the peaks or insufficient collector power, S-TAP or sniffer restarts, or too many sessions are coming into the collector. Priority packets are the packets that contain metadata responsible for correctly extracting session information. Partial loss of priority packets can cause interpretation issues such as mangled usernames, source program names, and other important session information. This example shows how to provide a check on the username to ensure that it is correct. If the username is not correct, the username is replaced by a user-defined value.
- [Login information dump example](#)  
Use the `login information dump` session level policy to help resolve Sniffer connection issues.

## Related tasks

---

- [Creating advanced session-level policies](#)
  - [Creating session-level policies](#)
- 

## Ignoring sessions example

The **Ignore sessions** policy shows two different methods of ignoring certain policies.

The **Ignore sessions** policy contains two rules:

- The first rule ignores sessions that meet specific criteria (client IP, server IP, and source program language).

You can include specific criteria in a group.

- - Example- You can include specific criteria in a group
- The second rule ignores invisible binary traffic, for example, background encrypted SSL or TLS sessions, which are useless but can overload the sniffer. Setting the Packets limit to 50 on the IGNORE SESSION rule action states that if the session does not encounter a query within the first 50 packets, then ignore the session.

Rule 1:

- Session level criteria:
  - Client IP address = 10.10.10.10
  - Server IP address = 20.20.20.20
  - Source application = JAVA%
- Rule action = *DISCARD SESSION*

Rule 2:

- Session level criteria: None
- Rule action: *IGNORE SESSION*  
Packets limit = 50

## SR language example

---

```
SR_POLICIES
{
 IF (CLIENT_IP = '10.10.10.10' SOURCE_PROGRAM = 'JAVA%' SERVER_IP = '20.20.20.20')
 {
 DISCARD_SESSION
 }
 IF (*)
 {
 IGNORE_SESSION PACKETS_LIMIT = 50
 }
}
```

## Related concepts

---

- [Audit and ignore session actions](#)

## Log LOGIN\_FAILED sessions only example

The **Log LOGIN\_FAILED sessions only** policy contains a single rule that logs an error if a login fails. Other types of errors that the session encounters are ignored.

This policy has one rule and one rule action.

- Session level criteria: Error != LOGIN\_FAILED
- Rule action = SOFT DISCARD

## SR language example

```
SR_POLICIES
{
 IF (ERROR != 'LOGIN_FAILED')
 {
 SOFT_DISCARD_SESSION
 }
}
```

## Related concepts

- [Search parameters](#)

## REQUEST\_ERROR example

REQUEST\_ERROR in the session level policies are SQL errors.

You can use it when you want to:

- Trigger the rule on any error request
- Identify sessions with too many user errors
- Identify errors while accessing specific tables

Variants for ERROR criteria:

```
ERROR = 'GUARDIUM://EMPTY' - No error code detected.
ERROR = '%' - Any error including Login failure.
ERROR = '<error code|LOGIN_FAILED>' - Specific error or Login failure.
ERROR = 'LOGIN_FAILED' - Login failure
```

Variants for REQUEST\_ERROR criteria:

```
ERROR = 'REQUEST_ERROR' - Any error excluding Login failure.
```

## Add DB name on failed login example

The **Add DB name on failed login** policy solves a problem where the database name is not available if the login fails (with a LOGIN\_FAILED message). If the DB NAME value is empty, the policy adds a database name.

This example has one rule and one rule action.

- Session level criteria:
  - Server IP address = 20.20.20.20
  - Server port = 1433
- Rule action = TRANSFORM\_DB\_NAME
  - Source = DB NAME
  - Request type = LOGIN FAILED
  - Output format = NEWACCDB

## SR language example

```
SR_POLICIES
{
 IF (SERVER_IP = '20.20.20.20' SERVER_PORT = '1433')
 {
 TRANSFORM_DB_NAME REQ_TYPE = LOGIN_FAILED OUTPUT_FORMAT = 'NEWACCDB'
 }
}
```

## Get correct service name (MS SQL Server) example

For MS SQL server, some sites use a placeholder name for the SERVICE\_NAME. This example shows how to replace the placeholder with the actual service name.

In the **Get correct service name** policy, the MS SQL server instance uses a placeholder name, MS SQL SERVER for the SERVICE\_NAME. The service name and the server hostname are concatenated into SERVER\_HOSTNAME, separated by a backslash (\). For example:

| SERVICE_NAME  | SERVER_HOSTNAME        |
|---------------|------------------------|
| MS SQL SERVER | MY_SQL_SERVICE\MY_HOST |

This example has one rule and two rule actions.

- Session level criteria:
  - Server IP address = 20.20.20.20
  - Database type = MS SQL SERVER

- Rule actions:

1. **TRANSFORM SERVICE NAME**

This rule finds all instances of SERVER HOSTNAME that contain a backslash. The output (for SERVER HOSTNAME) is the data after the backslash.

- Source = SERVER HOSTNAME
- Match pattern = (.\*)\\(.\*)
- Output format = |2

2. **TRANSFORM SERVER HOSTNAME**

This rule moves the first part of the original SERVER HOSTNAME and moves it to the SERVICE NAME.

- Source = SERVER HOSTNAME
- Match pattern = (.\*)\\(.\*)
- Output format = |1

The final output is as follows:

| SERVICE_NAME   | SERVER_HOSTNAME |
|----------------|-----------------|
| MY_SQL_SERVICE | MY_HOST         |

## SR language example

```
SR_POLICIES
{
 IF (DB_TYPE = 'MS SQL SERVER' SERVER_IP = '20.20.20.20')
 {
 TRANSFORM_SERVICE_NAME SOURCE = SERVER_HOST_NAME MATCH_PATTERN = '(.*)\\(.*)' OUTPUT_FORMAT = '\2'
 TRANSFORM_SERVER_HOST_NAME MATCH_PATTERN = '(.*)\\(.*)' OUTPUT_FORMAT = '\1'
 }
}
```

## Related concepts

- [Transform parameters](#)

## Ignoring exceptions examples

The **Ignoring exceptions** policy shows two ways to ignore certain exceptions.

Rule 1: Ignore TNS errors that are logged as LOGIN\_FAILED.

- Session level criteria
  - Server IP address in Group where,
    - Group type = Server IP
    - Members = IP addresses
  - Database type = ORACLE
  - Server port = 1521
- Rule action = IGNORE REQUEST
  - Request type = LOGIN FAILED
  - Search prefix = TNS-

Rule 2: Ignore error 42702, which is caused by multiple SQL DROP TABLE and CREATE TABLE command pairs.

- Session level criteria
  - Database type = DB2
- Rule action = IGNORE REQUEST
  - Request type = SQL
  - Search prefix = 42702

## SR language examples

While both of the exceptions are managed with a single policy in the UI, two SR language policies are needed.

Example 1:

```
SR_POLICIES
{
 IF (SERVER_IP = ('', 20005) SERVER_PORT = 1521 DB_TYPE = 'ORACLE')
 {
```

```

 IGNORE_REQUEST REQ_TYPE = LOGIN_FAILED SEARCH_PREFIX = 'TNS-'
 }

 GROUP_ID = 20005 TYPE = IP_ADDRESS SIZE = 2
 {
 '20.20.20.20' '30.30.30.30'
 }
}

```

Example 2:

```

SR_POLICIES
{
 IF (DB_TYPE = 'DB2')
 {
 IGNORE_REQUEST REQ_TYPE = SQL_ERROR SEARCH_PREFIX = '42702'
 }
}

```

## Related concepts

---

- [Audit and ignore session actions](#)

## Firewall and latency issues examples

If your site uses the Guardium® database firewall, you can encounter latency issues when Guardium reconnects. These examples show how to use session-level policies to prevent unwanted traffic.

In the following example, the application can automatically reconnect and restore a terminated session. In this case, a query that violates the rules is automatically sent at the begin of the session. Because the database firewall was too late, the violating query is sent to the database server.

In this example, the following steps occur within milliseconds:

1. The session is put under a firewall watch as soon as the user is verified in the analyzer.
2. The analyzer ends the session after the first query that contains the object CREDIT\_CARD.

The following session-level policy addresses this issue:

- Session level criteria:
  - Client IP address = 10.10.10.10
  - Client net mask = 255.255.255.0
  - Server IP address = 20.20.20.20
  - Database user = *Hermione*
  - Server port = 1521
- Rule actions:
  1. S-GATE SESSION ATTACH
    - ATTACH
    - ATTACH ON REQUEST
  2. S-GATE SESSION TERMINATE ON REQUEST
    - Request type = SQL
    - Search prefix = *SELECT*
    - Search pattern = *CREDIT\_CARD*

For the following example, Guardium attaches the session to the firewall for sessions when a database user tries to access database server objects for which they do not have permission. In this case, the Oracle database server issues error ORA-01031 – insufficient privileges.

Tip: Make sure that STAP\_FIREWALL\_DEFAULT\_STATE (Linux®-UNIX) or Firewall default state (Windows) S-TAP parameter is set to 2 to help prevent a security hole. If STAP\_FIREWALL\_DEFAULT\_STATE is set to 0 or 1, database clients that are not authorized by the security system database client can create database server sessions. A user can issue an SQL statement and the firewall reacts only after the first SQL statement (when a database session is already created).

The following session-level policy uses two rules to address this issue.

- Rule 1: Session level criteria
  - Server IP address = 20.20.20.20
  - Database user = *Bellatrix*
  - Server port = 1521
- Rule action = S-GATE SESSION ATTACH
  - Request type = *SQL ERROR*
  - Search prefix = *ORA-01031*
- Rule 2: Session level criteria
  - Server IP address = 25.25.25.25
  - Server port = 9160
- Rule action = S-GATE SESSION ATTACH ON REQUEST
  - Request type = *RPC*
  - Search prefix = *LOGIN*
  - Match pattern = *.\*bella.\*\$*

## SR language example

---

Example 1:

```

SR_POLICIES
{
 IF (CLIENT_IP = '10.10.10.10' CLIENT_NET_MASK = '255.255.255.0' SERVER_IP = '20.20.20.20' SERVER_PORT = 1521 DB_USER =
'Bellatrix')
 {
 VERDICT_ATTACH
 VERDICT_TERMINATE_REQ_TYPE = SQL SEARCH_PREFIX = 'SELECT' SEARCH_PATTERN = 'CREDIT_CARD'
 }
}

```

Example 2:

```

SR_POLICIES
{
 IF (SERVER_IP = '9.70.145.22' SERVER_PORT = 1521 DB_USER = 'SCOTT')
 {
 VERDICT_ATTACH REQ_TYPE = SQL_ERROR SEARCH_PREFIX = 'ORA-01031'
 }
}

```

## Related concepts

---

- [S-GATE actions \(Verdict actions\)](#)

## Related reference

---

- [Linux-UNIX: Firewall parameters](#)
- [STAP Control: Firewall details \(Windows\)](#)

## Sniffer overload issues examples

---

In some circumstances, the Guardium sniffer can be overloaded with unnecessary traffic. These three examples show how to prevent the traffic that can overload the sniffer, while still allowing other traffic through.

Example 1: Ignore any traffic from the SAP HANA statistics service.

- Session level criteria
  - Database type = *SAP HANA*
  - Source application = *STATISTICSERVICE*
- Rule action = *IGNORE SESSION*

Example 2: Optimized method to log only traffic from specified ports.

- Session level criteria - Server port *In Group* where:
  - Group type = *Server port*
  - Members = A list of the server ports to log.
- Rule action = *SELECT SESSION*

Example 3: Ignore traffic from Zabbix (a third-party product). This example requires three rules.

Rule 1 - If the session is not logged after 30 packets are received on the collector, then ignore this session.

- Session level criteria - No criteria
- Rule action = *IGNORE SESSION*
- Packets limit = 30

Rule 2 - Transform all dynamic source program strings that contain the phrase "ZABBIX" to the string ZABBIX.

- Session level criteria
  - Database type = *ORACLE*
  - Operating system user = *ZABBIX*
- Rule action = *TRANSFORM SOURCE PROGRAM NAME*
  - Source = *SOURCE PROGRAM NAME*
  - Match pattern = *.\*ZABBIX.\**
  - Output format = *ZABBIX*

Rule 3: Log any session where the source program is not ZABBIX. The first rule ignores the session if the session is not available within the first 30 packets. Since the session does not fall under the *SELECT\_SESSION* rule, it is not forwarded to the Logger and is ignored.

- Session level criteria - Source application = *ZABBIX*
- Rule action = *TRANSFORM SOURCE PROGRAM NAME*
  - Source = *SOURCE PROGRAM NAME*
  - Match pattern = *.\*ZABBIX.\**
  - Output format = *ZABBIX*

## SR language example

---

Example 1:

```

SR_POLICIES
{
 IF (DB_TYPE = 'SAP HANA' SOURCE_PROGRAM = 'statisticsService')
}

```

```

 {
 IGNORE_SESSION
 }
}

```

Example 2:

```

SR_POLICIES
{
 IF (SERVER_PORT = (1434, 1))
 { SELECT_SESSION }

 GROUP_ID = 1 TYPE = INTEGER SIZE = 3 { 1435 1436 1437 }
}

```

Example 3:

```

SR_POLICIES
{
 IF (*) { IGNORE_SESSION_PACKETS_LIMIT = 30 }

 IF (DB_TYPE = 'ORACLE' OS_USER = 'ZABBIX')
 {
 TRANSFORM_SOURCE_PROGRAM MATCH_PATTERN = '.*ZABBIX.*' OUTPUT_FORMAT = 'ZABBIX'
 }

 IF (SOURCE_PROGRAM == 'ZABBIX') { SOFT_DISCARD_SESSION }
}

```

## Related concepts

---

- [Audit and ignore session actions](#)
  - [Transform actions](#)
- 

## Query masking examples

Analyzer query masking can be useful when used with non-relational databases such as MongoDB or Cassandra, or protocol frameworks such as the Google protocol buffer or Apache Thrift. The following examples show how to mask unencrypted data in non-relational databases.

Example 1: Mask an unencrypted password from Cassandra.

- Session level criteria:
  - Server IP address = 20.20.20.20
  - Database type = CASSANDRA
- Rule action = *TRANSFORM STATEMENT*
  - Source = *STATEMENT*
  - Request type = *RPC*
  - Search prefix = *login*
  - Search pattern = *password*
  - Match pattern = *|x27|w+|x27|x7D|x7D|x29\$*
  - Mask = *True*
  - Output format = *|x27|x2A|x2A|x2A|x27|x7D|x7D|x7D|x29*

Example 2 : Mask the user credentials for a CouchBase REST query.

- Session level criteria: Server port *In Group* where:
  - Group type = *Server port*
  - Members = A list of server ports.
- Rule action = *TRANSFORM STATEMENT*
  - Source = *STATEMENT*
  - Request type = *SQL*
  - Search prefix = *\_CB POST /query/service*
  - Search pattern = *"pass": "*
  - Match pattern = *"pass": "[^"]{[^"]}\*[^"]"*
  - Mask = *True*
  - Output format = *"pass": "\*\*\*\*\*"*

## SR language examples

---

Example 1:

```

SR_POLICIES
{
 IF (SERVER_IP = '20.20.20.20' DB_TYPE = 'CASSANDRA')
 {
 TRANSFORM_STATEMENT REQ_TYPE = RPC SEARCH_PREFIX = 'login'
 SEARCH_PATTERN = 'password' MATCH_PATTERN = '\x27\w+\x27\x7D\x7D\x29$'
 MASK_OUTPUT_FORMAT = '\x27\x2A\x2A\x2A\x27\x7D\x7D\x29'
 }
}

```

Example 2:

```

SR_POLICIES
{
 IF (SERVER_PORT = (8091,100))
 {
 TRANSFORM_STATEMENT REQ_TYPE = SQL SEARCH_PREFIX = '_CB POST /query/service'
 SEARCH_PATTERN = '"pass":' MATCH_PATTERN = '"pass":[^"][^"]*'
 MASK_OUTPUT_FORMAT = '"pass":*****'
 }
 GROUP_ID = 100 TYPE = INTEGER SIZE = 1 { 8093 }
}

```

## Related concepts

---

- [Transform actions](#)

## Correct IP address (Oracle) example

When the Oracle connection manager handles the connection to the database server, the connection manager can insert the wrong IP address and other information. The following example shows how to ensure that Guardium has the correct information from Oracle.

This example has two rules.

Rule 1: If the session is not logged after 30 packets are received on the collector, then ignore this session.

- Session level criteria: No criteria
- Rule action = *IGNORE SESSION*
- Packets limit = 30

Rule 2: Map Oracle connection information correctly.

- Session level criteria:
  - Client IP address = *10.10.10.10*
  - Database type = *ORACLE*
  - Operating system user *In Group*, where:
    - Group type = *OS User*
    - Members = A list of allowed operating system users.
  - Server port = *1521*
  - Session = *LOCAL*
- Rule actions:
  - TRANSFORM SERVER HOST NAME*
    - Source = *SERVER HOST NAME*
    - Search prefix = *redwood*
    - Output format = *rh7u1-lenx01*
  - TRANSFORM ANALYZED CLIENT IP*
    - Source = *CLIENT HOST NAME*
    - Search prefix = *redwood*
    - Output format = *(.\*)*
  - TRANSFORM SERVER DESCRIPTION*
    - Source = *ANALYZED CLIENT IP*
    - Search prefix = *10*
    - Output format = *WITH ORACLE CONNECTION MANAGER*

## SR language example

---

```

SR_POLICIES
{
 IF (*) { IGNORE_SESSION_PACKETS_LIMIT = 30 }

 IF (CLIENT_IP = '10.10.10.10' SESSION = 'LOCAL' OS_USER = ('',1) DB_TYPE = 'ORACLE' SERVER_PORT = 1521)
 {
 TRANSFORM_SERVER_HOST_NAME SEARCH_PREFIX = 'redwood'
 OUTPUT_FORMAT = 'rh7u1-lenx01'

 TRANSFORM_ANALYZED_CLIENT_IP SEARCH_PREFIX = 'redwood'
 SOURCE = CLIENT_HOST_NAME OUTPUT_FORMAT = '(.*)'

 TRANSFORM_SERVER_DESC SEARCH_PREFIX = '10'
 SOURCE = ANALYZED_CLIENT_IP OUTPUT_FORMAT = 'WITH ORACLE CONNECTION MANAGER'
 }
 GROUP_ID = 1 SIZE = 1 { 'or18cl' }
}

```

## Related concepts

---

- [Audit and ignore session actions](#)
- [Transform actions](#)

## Show SQL schema names example

You can use a session-level policy to find and display an SQL schema name. This example shows how to move the schema name to the `GDM_CONSTRUCT_INSTANCE.APP_USER_NAME` table and column so that it is available for reports.

This policy contains one rule with two rule actions. The rule actions work as follows:

1. Copy the prefix `:SC=` and the value of DB USER into `GDM_CONSTRUCT_INSTANCE.APP_USER_NAME`.
2. Extract the schema name from SQL statements and copy it to `GDM_CONSTRUCT_INSTANCE.APP_USER_NAME` too.

Note: If the second rule action does not find the MATCH\_PATTERN, the policy does not override the result of the first action.

- Session level criteria:
  - Client IP address = 10.10.10.10
  - Server IP address = 20.20.20.20
  - Database type = SAP HANA
- Rule actions:
  1. `TRANSFORM APP USER NAME`
    - Source = `DB USER`
    - Output format = `:SC=(*)`
  2. `TRANSFORM APP USER NAME`
    - Source = `STATEMENT`
    - Request type = `SQL`
    - Search prefix = `SELECT`
    - Search pattern = `.M_DATABASE`
    - Match pattern = `.*(.*)\M_DATABASE`
    - Output format = `:SC=|1`

## SR language example

```
SR_POLICIES
{
 IF (CLIENT_IP = '10.10.10.10' SERVER_IP = '20.20.20.20' DB_TYPE = 'SAP_HANA')
 {
 TRANSFORM_APP_USER SOURCE = DB_USER OUTPUT_FORMAT = ':SC=(.*)'

 TRANSFORM_APP_USER REQ_TYPE = SQL SEARCH_PREFIX = 'SELECT' SEARCH_PATTERN = '.M_DATABASE'
 SOURCE = STATEMENT MATCH_PATTERN = '.*(.*)\M_DATABASE' OUTPUT_FORMAT = ':SC=|1'
 }
}
```

## Related concepts

- [Transform actions](#)

## Server and S-TAP IP addresses example

For some Guardium® implementations, one collector serves multiple S-TAPs. In some cases, customers want to have separate sets of session-level policies for each S-TAP. Normally they can use SERVER\_IP and SERVER\_NET\_MASK rule conditions. However, the server IP address can be different from STAP IP address. In these cases, use a session-level policy to associate the session-level policies by S-TAP.

You can manage this issue with either a group of IP addresses or by using a SENDER\_NET\_MASK. The two examples show both methods.

In the first example, the rule condition is set to check SENDER\_IP, which is the STAP IP address on the database server and to check that the database user is SCOTT.

If the conditions are met, the rule action is triggered. In this example, the action transforms the APP\_USER\_NAME in GDM\_CONSTRUCT\_INSTANCE table to match the SERVER\_HOSTNAME. In the OUTPUT\_FORMAT field, the action inserts the value SERVER\_HOSTNAME into the APP\_USER\_NAME field.

You can use a SENDER\_IP condition if you have multiple S-TAPs that are installed on the database server. Use the SENDER\_IP (which is the S-TAP IP address) to create a rule for one or more specified S-TAPs.

Specify S-TAP IP addresses in the GROUP of IP address. For example, to specify a single IP address in a group:

```
SENDER_IP = ('20.20.20.20',1)
```

Where: 1 is the number of members in the group.

For the second example, any NET\_MASK is triggered on the subnet in the group, rather than on a specific IP address (as described for the first example). For this example, the .20 IP address is related to SENDER\_IP, and .0 subnet IP is related to NET\_MASK condition.

Example 1: Use a group of IP addresses.

- Session level criteria:
  - Database User = `fred@example.com`
  - Server IP address In Group, where:
    - Group type = `Sender IP`
    - Members = A list of IP addresses.
- Rule actions:
  1. `TRANSFORM SOURCE PROGRAM NAME`
    - Source = `SOURCE PROGRAM NAME`
    - Search prefix = `Microsoft`
    - Output format = `GEORGE ODBC`
  2. `TRANSFORM SOURCE PROGRAM NAME`
    - Source = `SOURCE PROGRAM NAME`

- Output format = *GEORGE ODBC*

Example 2: Use a subnet mask:

- Session level criteria:
  - Server IP address *In Group*, where Group type = *Sender IP*  
Members = A list of IP addresses.
  - Subnet mask = 255.255.255.0
- Rule action: *TRANSFORM APP USER NAME*
  - Source = *SERVER HOST NAME*
  - Output format = (.\*)

## SR language examples

---

Example 1:

```
SR_POLICIES
{
 IF (SENDER_IP = ('20.20.20.1',1) DB_USER = 'fred@example.com')
 {
 TRANSFORM_SOURCE_PROGRAM SEARCH_PREFIX = 'Microsoft' OUTPUT_FORMAT = 'GEORGE ODBC'
 TRANSFORM_SOURCE_PROGRAM OUTPUT_FORMAT = 'GEORGE ODBC'

 }

 GROUP_ID = 1 TYPE = IP_ADDRESS SIZE = 8 #SENDER_IP GROUP
 {
 '20.20.20.2' '20.20.20.3' '20.20.20.4' '20.20.20.5' '20.20.20.6' '20.20.20.7' '20.20.20.8' '20.20.20.9'
 }
}
```

Example 2:

```
SR_POLICIES
{
 IF (SENDER_IP = ('20.20.20.20',1) DB_USER = 'SCOTT' SENDER_NET_MASK = '255.255.255.0')
 {
 TRANSFORM_APP_USER SOURCE = SERVER_HOST_NAME OUTPUT_FORMAT = '(.*)'

 }

 GROUP_ID = 1 TYPE = IP_ADDRESS SIZE = 2 #SENDER_IP GROUP
 {
 '20.20.20.1' '20.20.20.0'
 }
}
```

## Related concepts

---

- [Transform actions](#)

## User authentication (Oracle) example

---

If your site uses Oracle OS authentication, the DB\_USER cannot be captured in network traffic and therefore is not logged. For this session-level policy, if the DB\_USER is empty, the policy copies the ORACLE\_USER name to DB\_USER.

- Session level criteria:
  - Client IP address = 10.10.10.10
  - Server IP address = 20.20.20.20
  - Database type = *ORACLE*
  - Server port = 1521
- Rule action: *TRANSFORM DB USER*
  - Source = *OS USER*
  - Output format = (.\*)

## SR language example

---

```
SR_POLICIES
{
 IF (CLIENT_IP = '10.10.10.10' SERVER_IP = '20.20.20.20' DB_TYPE = 'ORACLE' SERVER_PORT = 1521)
 {
 TRANSFORM_DB_USER SOURCE = OS_USER OUTPUT_FORMAT = '(.*)'
 }
}
```

## Related concepts

---

- [Transform actions](#)

## Redacting data example

---

The REDACT rule action is similar to redaction in extrusion rules. Use REDACT to replace a matched pattern in SQL statements that are sent from client to server and mask the matched values.

In this example, any 13-16 digit number matches the regular expression and is masked by asterisks. The purpose is to mask credit card numbers, which usually meet the criteria.

- Session level criteria: None.
- Rule action: *Redact*
  - Data pattern =  $(\b(?\:\d[-]?)^{13,16}\b)$
  - Replacement symbol = *STAR\_SIGN*
  - 12.1 and later Replacement symbol = *Any*

Notes:

- The pattern to mask must be within parentheses ( ).
- The replacement symbol *STAR\_SIGN* is an asterisk (\*).
- 12.1 and later Along with the list of predefined replacement symbols, you can enter any custom symbol as a replacement symbol. If you enter multiple replacement symbols, then only the last symbol is used as the replacement symbol.

## SR language example

---

```
SR_POLICIES
{
 IF (*)
 {
 REDACT MATCH_PATTERN = '(\b(?\:\d[-]*?)^{13,16}\b)' REPLACEMENT_SYMBOL = STAR_SIGN
 }
}
```

## Related concepts

---

- [Extrusion actions](#)

## Hostname caching example

---

This example shows how to manage hostnames that are stored in a cache file, where the cache is updated hourly.

The cache is stored as *IP\_ADDRESS HOST\_NAME*. Use a TRANSFORM action to move the IP address in the cache to *HOST NAME*, which you can then use as the output value for all *IP\_ADDRESS TRANSFORM* actions.

- Session level criteria: None.
- Rule action: *TRANSFORM ANALYZED CLIENT IP*
  - Source = *CLIENT HOST NAME*
  - Search prefix = ?
  - Output format = (.\*)

## SR language example

---

```
SR_POLICIES
{
 IF (*)
 {
 TRANSFORM_ANALYZED_CLIENT_IP SEARCH_PREFIX = '?' SOURCE = CLIENT_HOST_NAME OUTPUT_FORMAT = '(.*)'
 }
}
```

## Related concepts

---

- [Transform actions](#)

## Ignore specified users example (MongoDB)

---

This example ignores all requests that belong to the MongoDB users NO\_AUTH and \_SYSTEM.

MongoDB allows users to connect to the database without authentication. When a user logs in, it is NO\_AUTH. If authentication never occurs, then it is just an extra record for each connection in the tables.

In another scenario, the user uses data security policies, which ignore S-TAP sessions.

In this case, the data security policy ignores the NO\_AUTH username. When the data security policy receives the real username, it is too late to ignore. This session-level policy avoids forwarding such connections only sessions to Logger, so the security policy does not ignore relevant sessions.

- Session level criteria:
  - Database user *Not in Group*, where Group type = *USERS*  
Members = A list of the users to ignore (that is, NO\_AUTH and \_SYSTEM).

- Subnet mask = 255.255.255.0
- Rule action: *SELECT SESSION*

## SR language example

---

```
SR_POLICIES {
 IF (DB_USER != ('',1) DB_TYPE = 'MONGODB')
 {
 SELECT_SESSION
 }
 GROUP_ID = 1 SIZE = 2
 {
 'NO_AUTH' '__SYSTEM'
 }
}
```

## Related concepts

---

- [Audit and ignore session actions](#)

## Scheduling with SESSION\_START examples

---

Use SESSION\_START to define when the session-level rules are active. The following examples show how to use the Session start time range parameter.

## SR language examples

---

Example 1: Ignore any session that starts outside of normal working hours (in this case after 7 PM and before 8 AM) and is labeled as a NIGHT\_JOB.

- Session level criteria:
  - Session start time range != [08:00..19:00]
- Rule action = *IGNORE REQUEST*
  - Request type = *SQL*
  - Search pattern = *NIGHT\_JOB*

Example 2: In many configurations, the database server and the collector are located in different time zones. For example, suppose that the database server is installed in San Francisco (Pacific time, which is UTC-8) and the collector is installed in Boston (Eastern Time, UTC-5). In this case, you need to specify both the session range and the time zone offset (as Coordinated Universal Time [UTC]).

- Session level criteria:
  - Session start time range = [08:00..19:00, -8]
- Rule action = *SELECT SESSION*

Example 3. Discard any session that runs between 8:00 PM and 8:30 PM that also meets all of the following criteria:

- The session comes from an S-TAP with IP address 25.25.25.25.
- The server port is 1422 (an MS SQL instance).
- The database user is Sirius.
- Session level criteria:
  - Database user = *Sirius*
  - Server port = 1433
  - Sender IP address = 25.25.25.25
  - Session start time range = [20:00..20:30]
- Rule action = *DISCARD SESSION*

## SR language examples

---

Example 1:

```
SR_POLICIES
{
 IF (SESSION_START = [08:00..19:00, -8])
 {
 SELECT_SESSION
 }
}
```

Example 2:

```
SR_POLICIES
{
 IF (SESSION_START != [08:00..19:00])
 {
 IGNORE_REQUEST REQ_TYPE = SQL SEARCH_PATTERN = 'NIGHT_JOB'
 }
}
```

Example 3:

```
SR_POLICIES
{
```

```

 IF (SENDER_IP = '25.25.25.25' SERVER_PORT = 1433 DB_USER = 'sirius' SESSION_START = [20:00..20:30])
 {
 DISCARD_SESSION
 }
}

```

## Related concepts

---

- [Audit and ignore session actions](#)

## Logging access activity for trusted sessions example

You can change LOG\_ACCESS\_ONLY functionality by using IGNORE\_REQUEST as shown in the following examples.

## SR language examples

---

The following example contains three if statements:

1. If the initial OS\_USER is ORACLE19, then transform the OS user from ORACLE19 to SIRIUS.
2. Log access only for all sessions where FRED is the database user.
3. If the OS\_USER is SIRIUS, stop logging access if any user runs a statement that contains \* FROM.

```

SR_POLICIES
{
 IF(OS_USER = 'ORACLE19')
 {
 TRANSFORM_OS_USER_SEARCH_PREFIX = '?' OUTPUT_FORMAT = 'SIRIUS'
 }
 IF(OS_USER = 'SIRIUS')
 {
 LOG_ACCESS_ONLY_SEARCH_PREFIX = 'DB_USER:FRED'
 }
 IF(OS_USER = 'SIRIUS')
 {
 STOP_LOG_ACCESS_ONLY_SEARCH_PREFIX = 'STATEMENT:/* FROM%'
 }
}

```

The following example performs a soft discard, with an option to revert the discard if sysdate is found in the sent statement.

The second action reverts the soft discard if any user runs a statement that contains \* FROM.

```

SR_POLICIES
{
 IF(*)
 {
 SOFT_DISCARD_SESSION_SEARCH_PREFIX = 'STATEMENT:sysdate'
 STOP_SOFT_DISCARD_SESSION_SEARCH_PREFIX = 'STATEMENT:/* FROM%'
 }
}

```

## Related concepts

---

- [Audit and ignore session actions](#)
- [Track option](#)

## Creating a custom exception message example

Create a custom exception message with the SR language THROW\_EXCEPTION or by selecting the LOG EXCEPTION action in the UI for a local session-level policy.

- Session level criteria:
  - Session = LOCAL
  - Database type = ORACLE
- Rule action = LOG EXCEPTION
  - Exception type = SECURITY INCIDENT
  - Exception message = *Restricted local connection \${SESSION\_INFO}\$*

Note: The exception message is logged only once per session.

## SR language examples

---

In the following example, if the analyzer encounters a PLAIN\_PASSWORD security incident, it logs a custom message.

```

SR_POLICIES
{
IF (INCIDENT = 'PLAIN_PASSWORD')
{
 THROW_EXCEPTION EXC_TYPE = SECURITY INCIDENT EXC_MSG = 'Unencrypted database connection'
}

```

```
 }
In this
```

## Related concepts

---

- [Exception actions](#)

## Find name in SQL query example

Create a session-level policy that sends an alert when a name is found in an SQL query.

You can use a session-level policy from the UI to create an alert when a name, or other specific information, is found in an SQL query.

- Session level criteria: Statement *In Group*, where Group type = *FIELDS*.  
Members = A list of the names for which you want to send an alert, for example:

```
%Jane%Doe%
%Doe%Jane%
```

- Rule action: *ALERT PER MATCH*
  - Message Template = *Default*
  - Notification Type = *SYSLOG*
  - Exception message = *DB user \$(DB\_USER)\$ has searched for name in database \$(DB\_NAME)\$*
  - Distinct = *blank*

## SR language examples

---

Alerts are not available in the SR language. To use the SR language to do a similar action, use the LIKE parameter and THROW\_EXCEPTION action, for example:

```
SR_POLICIES
{
 IF (STATEMENT LIKE ('', 20010))
 {
 THROW_EXCEPTION EXC_TYPE = SECURITY INCIDENT EXC_MSG = 'DB user (DB_USER) has searched for name in database
$(DB_NAME) $$'
 }

 GROUP_ID = 20010 SIZE = 2
 {
 '%Jane%Doe%' '%Doe%Jane%'
 }
}
```

## Related concepts

---

- [Alert and Log actions](#)
- [Exception actions](#)

## Detect local admin example

Use this policy to attach local admin sessions.

The following example uses a 1-parameter tuple. For more information about tuples, see [Tuples](#).

Session level criteria:

- Session *In Group*, where Group type = *Tuples*
  - Tuple parameters = *Session*
  - Members = A list of IP addresses
- Rule action: *S-GATE SESSION ATTACH*

## SR language example

---

```
SR_POLICIES
{
 TUPLES_GROUP_ID = 20008 TYPE = (SESSION) SIZE = 1
 {
 'ADMIN'
 }
 IF (TUPLES = ('', 20008) SESSION = 'LOCAL')
 {
 VERDICT_ATTACH
 }
}
```

## Related concepts

---

- [S-GATE actions \(Verdict actions\)](#)

## Strict username example (Oracle)

Monitoring network traffic is subject to network packet loss. Losses can occur for various reasons, such as overloading S-TAP buffers on the peaks or insufficient collector power, S-TAP or sniffer restarts, or too many sessions are coming into the collector. Priority packets are the packets that contain metadata responsible for correctly extracting session information. Partial loss of priority packets can cause interpretation issues such as mangled usernames, source program names, and other important session information. This example shows how to provide a check on the username to ensure that it is correct. If the username is not correct, the username is replaced by a user-defined value.

Note: This example is available only for Oracle databases.

This example has two rules.

Rule 1: ORACLE - Set the database type to Oracle and configure the STRICT\_USERNAME option.

- Session level criteria = Database type = *ORACLE*
- Rule action = CONFIGURE = *STRICT\_USERNAME:<replacement\_value>*  
Where *<replacement\_value>* is any value that you choose. If Guardium finds a problem with the username, it is replaced with the specified value.

Rule 2: Throw exception - Throw an exception if a problem is found with the username.

- - Session level criteria:
    - Database type = *ORACLE*
    - Session = *GET\_USERNAME\_PROBLEM*
  - Rule action = THROW EXCEPTION = *SESSION EXCEPTION*
  - Exception message = *Session \${SESSION\_INFO}\$. PROBLEM TO GET USERNAME. PLACEHOLDER USERNAME - \${DB\_USER}\$, CLIENT OS - \${CLIENT\_OS\_NAME}\$, SERVER OS - \${SERVER\_OS\_NAME}\$*

## Related concepts

- [Configure actions](#)
- [Exception actions](#)

## Login information dump example

Use the **login information dump** session level policy to help resolve Sniffer connection issues.

When you work with Guardium technical support to solve Sniffer issues, your support person might ask you to configure and run the slon looper or the **login information dump** session level policy. The slon looper and **login information dump** policy work together as follows.

The **login information dump** is a standard session-level policy template. To use this policy, click  to make a copy of the policy and make changes as needed. For example, you can specify a database username, an IP address, or other information.

Let's say that you have a scenario in which the username is empty, but packets aren't dropped in either the S-TAP or in Sniffer. One cause might be that the login sequence was encrypted or garbled and was sent more than 1 hour before the session's first statement. If the session received the login sequence, but timed out after an hour, then no information is available to log. In this case, the first incoming statement opens new session without login information and an error occurs. The **login information dump** session-level policy can help find these kinds of issues.

This example has two rules:

- Rule 1: Configure a login dump (CONFIGURE DUMP LOGIN)
  - Session level criteria: None.
  - Rule action: CONFIGURE Option =*DUMP\_LOGIN:ON*
- Rule 2: Create the login dump (DUMP LOGIN)
  - Session level criteria: None.
  - Rule action: LOG EXCEPTION = *SESSION EXCEPTION*
  - Exception message = *DUMP\_LOGIN:DUMP\_LOGIN: Session \${SESSION\_INFO}\$*

## SR language example

This example creates a login dump for an Oracle database.

```
SR_POLICIES
{
 IF (DB_TYPE = 'ORACLE')
 {
 CONFIGURE OPTION = 'DUMP_LOGIN:ON'
 }
 IF (DB_TYPE = 'ORACLE' STATEMENT LIKE 'BEGIN%')
 LOG EXC_TYPE = SESSION_EXCEPTION EXC_MSG = DUMP_LOGIN:DUMP_LOGIN: Session ${SESSION_INFO}$. Packets logged.
}
```

## Related tasks

- [Creating session-level policies](#)
- [Running the slon looper utility](#)

## Known limitations

The following known limitations apply to session-level policies and advanced session-level policies.

- Session-level policies apply on new database sessions opened after installing the session-level policy. When updating or removing session-level policies, existing sessions continue using the original policies until the sessions have finished their work.
- In some protocols, SERVICE\_NAME does not exist and is replaced by SERVER\_TYPE as a placeholder. For example, Microsoft SQL Server. In this case it is better to avoid using SERVICE\_NAME and to use DB\_TYPE instead.
- The Microsoft SQL Server username for local connections can be set to OS user and replaced later. Consider this when creating session-level policy rules.
- NET\_PROTOCOL can change during sessions and is not recommended for use.
- In rare cases, session information can be correlated in the logger (e.g. Oracle Kerberos authentication). Session parameters correlated in the logger should not be used as session-level policy rule conditions.
- When session-level policies use SQL criteria like command, object, literal or field, the following limitations apply:
  - The ANTLR3 parser is required.
  - Session-level policy processing is done on parsed context and constructs that do not have parser errors.
  - Some actions are not allowed with SQL criteria: TRANSFORM STATEMENT, NO PARSE, QUICK PARSE, QUICK PARSE NO FIELDS, MARK SESSION, CONFIGURE, LOG ACCESS ONLY, LOG EXCEPTION, and some TRANSFORM actions.
- Wildcards are allowed in session-level rule criteria, tuples, search parameters (except MATCH\_PATTERN), and groups (or LIKE groups when using advanced session-level policies). Regular expressions are allowed in rule criteria, groups and tuples. CIDR masking for IP addresses allowed in groups and tuples.
- IP address network masks are not applied to IP address groups. Mask IP address group members before creating the group and add them to the group in subnet form. If CLIENT\_NET\_MASK, SERVER\_NET\_MASK, or SENDER\_NET\_MASK used when CLIENT\_IP, SERVER\_IP, or SENDER\_IP contain a group, add the related subnet members directly to the group. Consider using CIDR notation in groups when it is needed.
- If session level policies are reinstalled, sessions are validated with the new policy rules.
- Regular expression use Perl syntax. The maximum size of regular expressions is 255 symbols. Note that Guardium checks regular expression syntax but does not check semantics. The regular expression language has advanced features and is recommended for use only by experienced users. Otherwise, regular expressions can lead to serious degradation of performance and available resources.
- Only one tuple per rule is allowed. Multiple tuples are allowed in the policy.
- For advanced session level policies only:
  - The size specified in the header of any group (including groups of tuples) must match the number of group member values specified in the body of the group. For example, in a six-tuple group with seven tuples, the seventh tuple will be disregarded.
  - Imported session rules only work with actions supported by advanced session level policies.
  - Advanced session level policies cannot be created with empty groups: at least one group member must be specified.
  - Importing session rules imports all currently installed session level policies and rules at once. If you need rules from a single policy, install that policy before importing so it will have only rules from that policy.
- Criteria ANALYZED\_CLIENT\_IP is the result of correlation encrypted and not encrypted sessions. This criteria is not always available.
- Rules that use the CONFIGURE action can use the following criteria: CLIENT\_IP\_ADDRESS, CLIENT\_NET\_MASK, SERVER\_IP\_ADDRESS, SERVER\_NET\_MASK, SERVER\_PORT, SENDER\_IP, SENDER\_NET\_MASK, DB\_TYPE, SESSION\_START\_TIME\_RANGE, NET\_PROTOCOL, SESSION(OPTIONS: LOCAL, TAP\_ENCRYPTED, ALL\_ENCRYPTED, W\_STAP, U\_STAP, E\_STAP, MID\_STREAM).
- For performance reasons, use fewer than 500 session-level rules across all installed policies.

## Policy rule actions

Define blocking, alerting, or logging actions to take when policy rules are matched.

Note: Consider that you have created a security policy that contains both access rules and extrusion rules. If the SQL request triggers the access rule actions and the SQL responses match the extrusion rules, you can use the [store skip extrusion on sql access rule match](#) CLI command to determine how or which extrusion rule actions may be skipped or executed. Use the CLI to help reduce duplicate logged data or alerts.

- [\*\*Blocking rule actions\*\*](#)  
This section describes S-TAP Terminate and S-GATE rule actions.
- [\*\*Alerting rule actions\*\*](#)  
Alert actions send notifications to one or more recipients.
- [\*\*Logging or ignoring rule actions\*\*](#)  
Logging actions control the level of logging based on the observed traffic.
- [\*\*Understanding ignore actions\*\*](#)  
Details about how data is handled when using ignore actions in policy rules.
- [\*\*Log full details\*\*](#)  
With log full details, Guardium logs data for each separate request and with unmasked values. Log full details also provides exact timestamps.
- [\*\*Set character set\*\*](#)  
You can use an action under a policy extrusion rule in order to attach alternative character sets to the session.
- [\*\*Rule definition fields\*\*](#)  
You can use these fields when you define policy rules.

## Blocking rule actions

This section describes S-TAP Terminate and S-GATE rule actions.

### S-TAP Terminate

The S-TAP Terminate action terminates a database connection (a session) and prevents additional requests on that session. This action is available in the S-TAP regardless of whether S-GATE is used.

Note: With S-TAP Terminate, the triggering request is not usually blocked but additional requests from that session are blocked. With a high request rate, sometimes more than one request may go through before the session is terminated.

## S-GATE

---

S-GATE provides database protection via the S-TAP for both network and local connections. When S-GATE is available, all database connections (sessions) are evaluated and tagged for monitoring in one of the following S-GATE modes:

- Attached (S-GATE is "on"): S-TAP is in firewalls mode for that session, and it holds the database requests and waits for a verdict on each request before releasing its responses. Latency is expected in this mode, but it ensures that rogue requests are blocked.
- Detached (S-GATE is "off"): S-TAP is in normal monitoring mode for that session, and it passes requests to the database server without any delay. Latency is not expected in this mode.

S-GATE configuration in the S-TAP itself defines the default S-GATE mode for all sessions, as well as other defaults related to S-GATE verdicts when the collector is not responding. For more information, see [Linux and UNIX systems: S-TAP firewall parameters](#) and [Windows: S-TAP firewall parameters](#).

It is possible to alter the default S-GATE configuration in real time using the following S-GATE policy rule actions:

- S-GATE Attach: sets S-GATE mode to "Attached" for a specific session. Intended for use when a certain criteria is met that raises the need to closely watch (and if needed block) the traffic on that session.
- S-GATE Detach: sets S-GATE mode to "Detached" for a specific session. S-GATE Detach is intended for use on sessions that are considered safe or sessions that cannot tolerate any latency.
- S-GATE Terminate: applies only when the session is attached, S-GATE Terminate drops the reply of the firewalled request and terminates the session on some databases. The S-GATE TERMINATE policy rule action causes a previously watched session to terminate.

Notes:

- S-TAP and S-GATE Terminate actions do not work on a client IP group whose members have wild-card characters. S-TAP and S-GATE Terminate only work with a single IP address. Wildcards should be handled by groups if the customer wants to use multiple IP entries. Customer can create groups of trusted or untrusted users/clients to handle their business needs in the policies.
- There are limitations for using S-GATE with A-TAP with older Linux kernels. For S-TAP V10.1.2 and higher, S-GATE is supported everywhere except Linux with A-TAP using kernels earlier than 2.6.36.
- For MySQL databases, the default command line connection is `mysql -u <user> -p <pass> <dbname>`. In this mode, MySQL first maps all the objects and fields in the database to support tab-key auto-completion. A terminate rule on any object or field involved in this mapping immediately disables the connection session. To avoid this, connect to MySQL with the `-A` flag, which disables the auto-complete feature and will not trigger the terminate rule. Another option is to fine-tune the rule and not terminate on any access to these objects or fields, instead defining a narrower criteria that does not trigger the rule on the login sequence.

---

## Alerting rule actions

Alert actions send notifications to one or more recipients.

For each alert action, multiple notifications can be sent, and the notifications can be a combination of one or more of the following notification types:

- Email messages: You can specify a Guardium user email, or an external email. Emails are sent using the SMTP server configured for the Guardium system. Additional receivers for email notification are the invoker (the user that initiated the actual SQL command that caused the trigger of the policy) and the owner (the owner of the database). The invoker and owner are identified by retrieving user IDs (IP-based) configured via Guardium APIs. To view these mappings, log in as `accessmgr` and go to Data Security > User-DB Association or use the `list_db_user_mapping` API command.
- SNMP traps: alerts the trap community configured for the Guardium system.
- Syslog messages: generates messages that are written to the syslog.  
Attention: The `%%RecordsAffected` variable does not return values when used in a message template for `alert only` rule actions that specify the `syslog` notification type.
- Custom notifications: user-created notification handlers implemented as Java classes.

Attention: Alert definitions and notifications are not subject to data-level security for the following reasons: alerts are not evaluated in the context of users, alerts may be related to databases associated with multiple users, and to avoid situations where no one receives the alert notification.

---

## Alert messages

The contents of an alert are defined by message templates. Navigate to Setup > Global Profile, locate the Named template field, and click Edit. Use the Named Template Finder to create, review, and modify message templates.

---

## Alert behaviors

There are several types of alert actions, including the following:

- Alert Daily: sends notifications only the first time the rule is matched each day.
- Alert Once Per Session: sends notifications only once for each session in which the rule is matched. This action might be appropriate in situations where you want to know that a certain event has occurred, but not for every instance of that event during a single session. For example, you may want a notification sent when a certain sensitive object is updated, but if a program updates thousands of instances of that object in a single session, you would not want thousands of notifications sent to the receivers of the alert.
- Alert Only: when Alert Only is used with the syslog notification type, messages go directly to `/var/log/messages`. For other notification types, Alert Only sends messages to the MESSAGE table. Alert Only does not notify of policy violations.  
Attention: The `%%RecordsAffected` variable does not return values when used in a message template for `alert only` rule actions that specify the `syslog` notification type.
- Alert Per Match: sends notifications each time the rule is satisfied. This is appropriate for a condition requiring attention each and every time it occurs.
- Alert Per Time Granularity: sends notifications once per logging granularity period. For example, if the logging granularity is set to one hour, notifications are sent for only the first match of the rule during each hour.

Tip: The Guardium administrator sets logging granularity using the [Manage > Activity Monitoring > Inspection Engines](#) tool.

## Related concepts

- [The alert message template](#)

## Logging or ignoring rule actions

Logging actions control the level of logging based on the observed traffic.

Access rules, exception rules, and extrusion rules differ in which actions are available. For example, Log and Ignore actions are available for most policies, but the Audit Only action is only available for policies that use the Selective Audit Trail setting.

### Audit Only

This action is only available for policies that use the Selective Audit Trail setting.

Audit Only logs the construct that triggered the rule. For a Selective Audit Trail policy, no constructs are logged by default, so use this selection to indicate which constructs you want to log. For example, for the Application Events API, if you want to log database usernames for reporting, use this action (otherwise, in this example, the username is blank).

### Allow

When matched, log the matching construct but do not log a policy violation. If the Allow action is selected, no other actions can be added to the rule.

### Log Only

Log the policy violation. Except for the Allow action, a policy violation is logged each time that a rule is triggered unless the rule action suppresses logging.

### Log Masked Details

This action is available for access rules and extrusion rules.

Log the full SQL for the request, replacing values with question marks (?).

### Log Full Details

Log the full SQL string and the exact timestamp for the request.

### Log Full Details with Values

Like Log Full Details, but each value is stored as a separate element such that the values are parsed and logged in to a separate table in the database. This log action uses more system resources as it logs the specific values of the relevant commands. Use this log action only when you need to generate reports with specific conditions on these values.

Attention: Consult technical services to access this log action.

### Log Full Details per Session

Log the full SQL string and exact timestamp for this request and for the remainder of the session.

### Log Full Details with Values per Session

See the descriptions for Log Full Details with Values and Log Full Details per Session.

Attention: Consult technical services to access this log action.

### Skip Logging

When matched, do not log a policy violation and stop logging constructs. This action is similar to the Allow action, but it also stops the logging of constructs. This action is used to eliminate the logging of constructs for requests that are known to be of no interest. This feature also applies for exception rules that concern database error codes only, allowing users to not log errors when an application generates a large and unavoidable quantity of errors.

Note: GDM\_CONSTRUCT is logged sometimes because parsing and logging of the construct occurs before the rule is applied, but the construct is included in the session.

### Ignore Responses per Session

Responses for the remainder of the session are ignored. This action does not log a policy violation, but it stops analyzing responses for the remainder of the session. This behavior is useful in cases where you know that the database response is of no interest. This action works when data is sniffed from an S-TAP, but it does not work when data is sniffed from a SPAN port.

Note: For Ignore Responses per Session, since the sniffer does not receive any response for the query or it is ignored, the values for COUNT\_FAILED and SUCCESS are the default. In this case, the values are COUNT\_FAILED=0 and SUCCESS=1.

### Ignore Session

The current request and the remainder of the session are ignored. This action does not log a policy violation. But it stops the logging of constructs and does not test for policy violations of any type for the remainder of the session. This action might be useful if the database includes a test region and you do not need to apply policy rules against that region of the database. The S-TAP or sniffer discards or disregards activity from individual sessions due to the execution of an ignore session rule action.

Important: Connection (login and logout) information is always logged, even if the session is ignored.

### Ignore S-TAP Session

The current request and the remainder of the S-TAP session are ignored. This action is done in combination with specifying specific systems, users, or applications that are producing a high volume of network traffic. This action is useful in cases where you know that the database response from the S-TAP session is of no interest.

- If no SQL is recorded for a session, then the "Ignore S-TAP Session" NEVER fires - and hence the **Session:Session Ignored** flag is recorded as No.
- If a session has 1 or more SQL statements, then the **Session:Session Ignored** flag recorded as Yes.

Use Ignore S-TAP Session as follows:

- IGNORE S-TAP SESSION: A "hard" ignore that cannot be revoked.
  - IGNORE STAP SESSION (REVOCABLE): A "soft" ignore; this rule action can enable the session traffic to be sent again without requiring a new connection to the database.
  - REVOKE Ignore - Resumes the sessions that are ignored by IGNORE\_S-TAP\_SESSION (REVOCABLE) action, which means that traffic is sent to the Guardium system after the S-TAP receives the **REVOKE Ignore** command. This command is sent from the S-TAP Control page using Revoke All Ignored Sessions.
- Note: The Revoke Ignore command persists for the S-TAP host in one sniffer process. New sessions opened after the S-TAP is in the revoked ignore state are not ignored even if the rule IGNORE\_STAP\_SESSION (REVOCABLE) is triggered.

Tip: Use IGNORE S-TAP SESSION (REVOCABLE) only when some of your IGNORE S-TAP SESSION actions need to be revoked. Otherwise, use IGNORE S-TAP SESSION because it's simpler and faster.

#### Ignore SQL per Session

Do not log SQL for the remainder of the session. Exceptions are still logged, but the system might not capture the SQL strings that correspond to the exceptions.

#### Log Extrusion Counter

This action is only available for extrusion rules.

Update the counter but do not log any of the returned data. This action saves disk space when the counter value is more important than the returned values.

#### Log Masked Extrusion Counter

This action is only available for extrusion rules.

Update the counter and log the SQL request, replacing values with question marks (?). This action does not log the returned values.

#### Quarantine

This action is available for access, exception, and extrusion rules.

Prevent the same user from logging in to the same server for a specified time period. To use the Quarantine rule action, you must also specify a duration for the quarantine with the Quarantine for (minutes) setting. If the session is watched (S-GATE), the action sends a drop verdict. If the session is not watched (S-TAP Terminate), the action has the S-TAP stop the session.

Quarantine timestamps are calculated by taking the current time and adding the number of minutes from the reset interval field. The new timestamp, which is sorted by timestamp, is kept in a structure along with server IP, server type, DB username, service name, and a flag that indicates whether the session is watched.

#### No Parse

Do not parse the SQL statement.

#### Quick Parse

This action is for access rules.

Do not parse the SQL statement for the remainder of the session. This action reduces parsing time. In this mode, all objects that are accessed can be determined but the exact object instances are unknown.

#### Note:

If you are using the universal connector, this action is only available for plug-ins that delegate the language syntax parsing to Guardium Data Protection. These cases usually occur when Guardium Data Protection supports that language natively. This action is not available if you are using a plug-in that parsed the language syntax by itself and does not delegate the syntax parsing to Guardium Data Protection.

#### Quick Parse No Fields

Do not parse fields in the SQL statement. Quick parse rules are only applied if SQL string is greater than 100 characters.

#### Quick Parse Native

This action is used only for Guardium S-TAP for Db2 on z/OS.

Use this rule action to improve performance in an environment where heavy traffic is overloading the Guardium sniffer.

#### Redact

This action is for extrusion rules.

Mask portions of database query output in reports for certain users, for example credit card numbers. Define the masking character by the Replacement character of the Data pattern parameter of the extrusion rule. If output produced by the extrusion rule matches the regular expression of the Data pattern, the portions that match subexpressions between parenthesis ( and ) are replaced by the masking character. Predefined regular expressions can also be used. For more information, see Data Pattern in [Rule definition fields](#).

#### Restriction:

- Redaction does not work on open sessions after an S-TAP live upgrade.
- Redaction does not work on tables that are created with field and number type.
- Redaction is available only with unencrypted traffic.
- Redaction is supported only with ANSI character sets.
- Delay in redaction is proportional to the amount of data returned by the query.
- The following restrictions apply only to regular (non-session-level) policies:
  - SQL Pattern is not supported for redaction rules.
  - Set redaction rules on the session level (attributes like IP addresses or users) and not on the SQL level (attributes like OBJECT\_NAME or VERB). If you set redaction rules on the SQL that needs to be scrubbed, it can take a few milliseconds for the scrub instructions to reach the S-TAP. In this case, some results might go though unmasked.

To guarantee that all SQL is redacted, set the S-TAP's default S-GATE mode to "attach" for all sessions that use the guard\_tap.ini file. This step guarantees that the rules engine, which holds each request and waits for the policy's verdict on the request, inspects all commands. This deployment introduces some latency but makes sure that data is 100% scrubbed.

In the Informix database, when you use char data type, columns do not have null termination at the end. All four columns are captured in the sendmsg system call as one piece, and K-TAP always tries to redact whatever data it captures. This behavior is a limitation when you use redaction with Informix.

- For more information about issues with redact, see the troubleshooting tips under [Policies](#).

#### Record Values Separately

#### Do Not Record Values Separately

This action is a session-based access rule. Used in replay functions to distinguish between transactions.

#### Mark as Auto-commit ON

#### Mark as Auto-commit OFF

This action is a session-based access rule. Used in replay function due to various auto-commit models for different databases.

#### z/OS Audit

This action is used only for datasets, Db2, and IMS collection profile policy rules that specify which traffic to collect on a z/OS server.

Traffic that meets the filtering criteria is sent to the collector. Only this action can be specified on a collection profile rule.

## Understanding ignore actions

Details about how data is handled when using ignore actions in policy rules.

#### Ignore session

The current request and the remainder of the session will be ignored. This action does not log a policy violation, but it stops the logging of constructs and will not test for policy violations of any type for the remainder of the session. This action might be useful if, for example, the database includes a test region, and there is no need to apply policy rules against that region of the database.

Table 1. Ignore session

| Data logged or ignored between client and DB Server/S-TAP | Data sent from DB Server/S-TAP to Collector                                                                                                                                                                                                              | Data from Span Port/ Network TAP to Collector                                                                                                  |
|-----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Ignore - SQL commands, SQL errors, Result Sets            | Log in/ Log out<br>Sniffer to S-TAP - One signal to S-TAP to stop sending activity for this session. If additional activity is sent by S-TAP, it is ignored at the sniffer level only.<br>Ignore SQL commands<br>Ignore SQL errors<br>Ignore Result Sets | Ignore – SQL commands, SQL errors, Result Sets.<br>SQL commands and errors coming from a Span Port or Network TAP are filtered at the Sniffer. |

#### Ignore S-TAP session

The current request and the remainder of the S-TAP session will be ignored. This action is done in combination with specifying in the policy builder menu screen of certain machines, users or applications that are producing a high volume of network traffic. This action is useful in cases where you know the database response from the S-TAP session will be of no interest.

Table 2. Ignore S-TAP session

| Data logged or ignored between client and DB Server/S-TAP | Data sent from DB Server/S-TAP to Collector                                                                                                                             | Data from Span Port/ Network TAP to Collector                                                                     |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Ignore - SQL commands, SQL errors, Result Sets            | Log in/ Log out Sniffer to S-TAP - One signal to S-TAP to stop sending activity for this session. Additional signals to S-TAP to stop sending activity to this session. | Not Applicable<br>If there is a need to ignore traffic from a Span Port/ Network TAP, use Ignore session instead. |

#### 12.1 and later Ignore responses per session

Responses for the remainder of the session will be ignored. This action does not log a policy violation, but it stops analyzing responses for the remainder of the session. This action is useful in cases where you know the database response will be of no interest.

Note: For ignore response per session, since the sniffer does not receive any response for the query or it is ignored, then the values for COUNT\_FAILED and SUCCESS are whatever the default for the table says they are, in this case COUNT\_FAILED=0 and SUCCESS=1.

Table 3. Ignore responses per session

| Data logged or ignored between client and DB Server/S-TAP | Data sent from DB Server/S-TAP to Collector                                                                                                                                          | Data from Span Port/ Network TAP to Collector                     |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| Log – SQL commands Ignore - SQL errors, Result Sets       | Log in/ Log out SQL Commands Sniffer to S-TAP - One signal to S-TAP to stop sending activity for this session. Additional signals to S-TAP to stop sending activity to this session. | Not applicable<br>This rule action is S-TAP-only implementations. |

#### Ignore SQL per session

No SQL will be logged for the remainder of the session. Exceptions will continue to be logged, but the system may not capture the SQL strings that correspond to the exceptions.

Table 4. Ignore SQL per session

| Data logged or ignored between client and DB Server/S-TAP | Data sent from DB Server/S-TAP to Collector                                                                                                                                                                                                 | Data from Span Port/ Network TAP to Collector                              |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Ignore - SQL commands                                     | Log in/ Log out                                                                                                                                                                                                                             | Ignore – SQL commands                                                      |
| Log - SQL errors, Result Sets                             | Sniffer to S-TAP - One signal to S-TAP to stop sending activity for this session. If additional activity is sent by S-TAP, it is ignored at the sniffer level only.<br>SQL commands<br>SQL errors<br>Result Sets, if using extrusion rules. | Log - SQL errors, Result Sets<br>SQL commands are filtered at the Sniffer. |

#### Selective Audit Trail

Use a Selective Audit Trail policy to limit the amount of logging on the appliance. This is appropriate when the traffic of interest is a relatively small percentage of the traffic being accepted by the inspection engines, or when all of the traffic you might ever want to report upon can be completely identified.

It is important to note that Ignore Session rules are still very important to include in the policy even if using a Selective Audit Trail. Ignore Session rules decrease the load on a collector considerably because by filtering the information at the S-TAP level, the collector never receives it and does not have to consume resources analyzing traffic that will not ultimately be logged. A Selective Audit Trail policy with no Ignore Session rules would mean that all traffic would be sent from the database server to the collector, causing the collector to analyze every command and result set generated by the database server.

Table 5. Selective Audit Trail

| Data logged or ignored between client and DB Server/S-TAP | Data sent from DB Server/S-TAP to Collector                                                                                                           | Data from Span Port/ Network TAP to Collector                              |
|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Ignore - SQL commands                                     | Log in/ Log out                                                                                                                                       | Ignore – SQL commands                                                      |
| Log - SQL errors, Result Sets                             | Ignore SQL commands, except for those defined by Audit-Only or Log Full Details rules.<br>Log SQL errors<br>Log Result Sets, if using extrusion rules | Log - SQL errors, Result Sets<br>SQL commands are filtered at the Sniffer. |

## Log full details

With log full details, Guardium logs data for each separate request and with unmasked values. Log full details also provides exact timestamps.

By default the Guardium® collector masks all values when logging an SQL string. For example

```
insert into tableA (name,ssn,ccn) values ('Bob Jones', '429-29-2921','29249449494949494')
```

is logged as `insert into tableA (name,ssn,ccn) values (?, ?,?)`. This is the default behavior for two reasons:

1. Values should not be logged by default because they may contain sensitive information.
2. Logging without values can provide for increased system performance and longer data retention within the appliance. Very often, database traffic consists of many SQL requests, identical in everything except for their values, repeated hundreds, thousands, or even millions of times per hour. By masking the values, Guardium is able to aggregate these repeated SQL requests into a single request, called a "construct". When constructs are logged, instead of each individual SQL request/construct being logged separately, it is only logged once per hour (per session) with a counter of how many times the construct was executed. This can save a tremendous amount of disk space because, instead of creating a hundreds (or millions) of lines in the database, only one new line is added.

With Log Full Details, Guardium logs the data with the values unmasked and each separate request. Log Full Details also provides the exact timestamp whereas logging without details provides the most recent timestamp of a construct within the logging granularity time period (usually 1-hour).

Important: When using log full details, if the inspection engine is not configured with inspect returned data enabled, the success or failure of SQL statement is not updated correctly. For more information about configuring inspection engines to inspect returned data, see [Inspection Engine Configuration](#).

Ignore S-TAP Session - Ignore S-TAP Session causes the collector to send a signal to the S-TAP instructing it to stop sending all traffic, except for the logout notification, for specific sessions. For example, if you have a rule that says `where`

```
DBUserName?=?scott, Ignore S-TAP Session:
```

- When Scott logs into the database server, S-TAP sends the connection information to the collector.
- The collector logs the connection. Session information (log in/log outs) are always logged.
- The collector sends a signal to S-TAP to stop sending any more traffic from this specific session. This means that any commands run by Scott against the database server and any responses (result sets, SQL errors, etc.) sent by the Database server to Scott will be discarded by S-TAP and will never reach the collector.
- When Scott logs out of the database server, S-TAP will send this information to the collector (log in/log out information is always tracked even if the session is ignored).
- When Scott logs in again, these steps are repeated. The logic on which sessions should be ignored is maintained by the collector, not the S-TAP.

It is important to note that Ignore Session rules are still very important to include in the policy even if using a Selective Audit Trail. Ignore Session rules decrease the load on a collector considerably because by filtering the information at the S-TAP level, the collector never receives it and does not have to consume resources analyzing traffic that will not ultimately be logged. A Selective Audit Trail policy with no Ignore Session rules would mean that all traffic would be sent from the database server to the collector, causing the collector to analyze every command and result set generated by the database server.

## Using MS-SQL or Sybase batch statements

There is a limitation where the success or failure of SQL commands in MS-SQL or Sybase batch statements may not show correctly.

MS-SQL or Sybase SQL batch statements are primarily used when creating complex procedures. When executing SQL statements separately, the status of each statement is tracked separately and will have the correct success or failure value. However, when a batch of SQL statements (used in MS-SQL or Sybase) are executed together, the status returned is the single status of the last transaction in the batch.

For example:

```
[Start of SQL batch]
SQL 1 statement - failed
SQL 2 statement - failed
SQL 3 statement - success
[End of SQL batch]
```

In the Guardium application, only the success or failure of the last SQL statement is reported in a MS-SQL or Sybase batch statement. In this case, success is reported for the MS-SQL or Sybase batch statement, even though SQL 1 and SQL 2 failed.

## Set character set

You can use an action under a policy extrusion rule in order to attach alternative character sets to the session.

Example of extrusion rule (with hint):

Character set EUC-JP (code 274).

Extrusion rule pattern: `guardium://char_set?hint=274`

As a result an extrusion rule is attached to the session and Analyzer will use EUC-JP in the session, if there is no other character set.

Example of extrusion rule (with force) :

Character set EUC-JP (code 274).

Extrusion rule pattern: `guardium://char_set?force=274`

As a result an extrusion rule us attached to the session and Analyzer will use EUC-JP character set in the session in any case. Character set used before will be substituted by EUC-JP.

Keep in mind that extrusion rules usually attach to the session with some delay. Therefore short sessions or the beginning of the session are not immediately changed by a character set change. The schema works for: Oracle, Sybase, MY SQL, and MS SQL.

## Rule definition fields

You can use these fields when you define policy rules.

Table 1. Reference Table of Rule Definition Fields

| Field                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action                                                   | Indicates the action to be taken when the rule is true. For a comprehensive description of all rule actions, see Rule Actions Overview.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| App Event Exists                                         | Match for an application event only. See the App Event Note.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| App Event Values                                         | Match the specified application event Text, Numeric, or Date values. Also allow a Group to be chosen for the event string as an option. See the App Event Note.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| (App) Event Type                                         | Match the specified application event. See the App Event Note.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| (App) Event User Name                                    | Match the specified application event username only. See the App Event Note.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| App Event Note                                           | The App Event fields cannot be used when the Flat Log box is marked.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| App. User                                                | Application User. For more information, see <a href="#">Values and groups of values in rules</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Category                                                 | An arbitrary label that can be used to group policy violations for reporting purposes. A default category can be specified in the policy definition, but the default can be overridden for each rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Classification                                           | An arbitrary label that can be used to group policy violations for reporting purposes. A default classification can be specified in the policy definition, but the default can be overridden for each rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Client Info                                              | DB2® client information: For access rules only. For z/OS® only, a CLIENT INFO field (and CLIENT_INFO_GROUP_ID) is visible if DB_TYPE is either Db2, Db2 COLLECTION Profile or VSAM COLLECTION Profile.<br><br>The type of information that can be placed in this field is USER=x; WKSTN=y; APPL=z.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Client IP                                                | <p>Clear the Not box to include, or mark the Not box to exclude:</p> <ul style="list-style-type: none"> <li>Any client: Leave all client fields blank. The count is incremented every time that any client satisfies the rule. (You cannot leave all fields blank if the Not box is marked.)</li> <li>All clients that are selected by an IP address and mask: Enter a client IP address in the first box and network mask in the second box. The count is incremented each time that any of the specified clients satisfies the rule. For example, to select all clients in subnet 192.168.9.x, enter 192.168.9.1 in the first box and 255.255.255.0 in the second box.</li> <li>A group of clients: Select a group of client IP addresses from the Group list, or click Groups to define a new group and then select that group. The count is incremented each time that any member of the selected group satisfies the rule.</li> <li>All clients that are selected by an IP address and mask AND a group of clients: Use both the Client IP and Group fields. The count is incremented each time that any client is specified who uses either method that satisfies the rule.</li> </ul> <p>Allow wildcard in IP address. Wildcard % is permitted in a policy for Client IP group.</p> |
| Client IP/Source Program/DB User/ Server IP/Service Name | <p>7-tuple group - Client IP/Src App/DB User/Server IP/Svc. Name/OS User/DB<br/>5-tuple group type available for access, exception, and extrusion rules.<br/>A tuple allows multiple attributes to be combined together to form a single group member.<br/>Tuple supports the use of one slash and a wildcard character (%). It does not support the use of a double slash.<br/>Wildcard % is permitted in a policy for Client IP/Source Program/DB User/ Server IP/Service Name group.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Client MAC                                               | <p>To make the rule sensitive to a single client MAC address, you can take one of the following steps:</p> <ul style="list-style-type: none"> <li>Enter the address in nn:nn:nn:nn:nn:nn format, where each n is a hexadecimal digit (0-F).</li> <li>Enter a dot (.) in the Client MAC box to indicate to maintain a separate count for each client MAC address.</li> <li>Leave the Client MAC box empty to ignore client MAC addresses.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Command                                                  | <p>The command. You can have situations in which a command group cannot be edited, and the and/or Group label changes to Collect Only, indicating that commands from only the selected group are to be selected. For more information, see <a href="#">Values and groups of values in rules</a>.</p> <p>If the Every member in group option is selected, all fields of the SQL statement must be a member of the defined group. However, the SQL statement does not need to contain all members of the group. For example, for the group <b>DB_TABLES_PROD</b> with members <b>students</b>, <b>module</b>, <b>marks</b>:</p> <ul style="list-style-type: none"> <li>For the query <b>select * from students;</b>, the object <b>students</b> is in the group and triggers the rule.</li> <li>For query <b>select * from students, module, marks;</b>, all three objects are in the group, which triggers the rule.</li> <li>For the query <b>select * from students, test;</b>, the object <b>test</b> is not in the group and does not trigger the rule when the Every member in group option is selected. However, it triggers the rule if the In group option is selected, since <b>students</b> is a member of the group.</li> </ul>                                                  |
| Continue to Next Rule                                    | If marked, rule testing will continue with the next rule, regardless of whether this rule is satisfied. This means that multiple rules can be satisfied (and multiple actions taken) by a single SQL statement or exception. If not marked (the default), no additional rules are tested for the current transaction when this rule is satisfied.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Field                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                        |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|----------|------------|----------------|-------------|----------------|-------------------|-------------|----------------|----------------------|---------------------|------------------------|-------------------------|---------------------|------------------------|---------------------|-----------------|----------------|------------------------|------------------|----------------|------------------------|-----------------|----------------|---------------------------|----------------|----------------|--------|----------|------------|----------------|-------------|----------------|-------------------|-------------|----------------|----------------------|---------------------|----------------|-------------------------|---------------------|----------------|---------------------|-----------------|----------------|------------------------|------------------|----------------|-----------------------|-----------------|----------------|--------------------------|------------------|----------------|
| Data Pattern              | <p>Every type of rule (Access, Exception, Extrusion) can have Data pattern, but it is required for Extrusion rules.</p> <p>For use in defining Extrusion Rules - A regular expression to be matched, in the Data Pattern box. Click Regex to open the Build Regular Expression tool, which allows you to enter and test regular expressions. This enables more complex masking patterns. Put parentheses around the section that you want to mask. Use this function to mask data retrieved from the database.</p> <p>For example,</p> <pre><b>Windows S-TAP:</b> ([0-9][0-9][0-9][0-9[-, ]?[0-9][0-9][0-9][0-9][-, ]?[0-9][0-9][0-9][0-9][-, ]?) [0-9][0-9][0-9][0-9][0-9]</pre> <pre><b>Unix S-TAP:</b> ([0-9]{4}[-, ]?[0-9]{4}[-, ]?[0-9]{4}[-, ]?) [0-9]{4}[ ]{0,20}</pre> <p>Additional regular expressions (Regex) for use only in Data Patterns with an action of Redact (Scrub):</p> <pre><b>For Windows S-TAP</b></pre> <table border="1"> <thead> <tr> <th>Name :</th> <th>Pattern:</th> <th>Masked to:</th> </tr> </thead> <tbody> <tr> <td>SCRUB_SSN_ANSI</td> <td>AAA-AA-AAAA</td> <td>****-****-AAAA</td> </tr> <tr> <td>SCRUB_SSN_UNICODE</td> <td>UUU-UU-UUUU</td> <td>****-****-UUUU</td> </tr> <tr> <td>SCRUB_CC_SPACES_ANSI</td> <td>AAAA AAAA AAAA AAAA</td> <td>***** ***** ***** AAAA</td> </tr> <tr> <td>SCRUB_CC_SPACES_UNICODE</td> <td>UUUU UUUU UUUU UUUU</td> <td>***** ***** ***** UUUU</td> </tr> <tr> <td>SCRUB_CC.Solid_ANSI</td> <td>AAAAAAAAAAAAAAA</td> <td>**********AAAA</td> </tr> <tr> <td>SCRUB_CC.Solid_UNICODE</td> <td>UUUUUUUUUUUUUUUU</td> <td>**********UUUU</td> </tr> <tr> <td>SCRUB_CC_AX.Solid_ANSI</td> <td>AAAAAAAAAAAAAAA</td> <td>**********AAAA</td> </tr> <tr> <td>SCRUB_CC_AX.Solid_UNICODE</td> <td>UUUUUUUUUUUUUU</td> <td>**********UUUU</td> </tr> </tbody> </table><br><pre><b>UNIX S-TAP</b></pre> <table border="1"> <thead> <tr> <th>Name :</th> <th>Pattern:</th> <th>Masked to:</th> </tr> </thead> <tbody> <tr> <td>SCRUB_SSN_ANSI</td> <td>AAA-AA-AAAA</td> <td>****-****-AAAA</td> </tr> <tr> <td>SCRUB_SSN_UNICODE</td> <td>UUU-UU-UUUU</td> <td>****-****-UUUU</td> </tr> <tr> <td>SCRUB_CC_SPACES_ANSI</td> <td>AAAA AAAA AAAA AAAA</td> <td>**********AAAA</td> </tr> <tr> <td>SCRUB_CC_SPACES_UNICODE</td> <td>UUUU UUUU UUUU UUUU</td> <td>**********UUUU</td> </tr> <tr> <td>SCRUB_CC.Solid_ANSI</td> <td>AAAAAAAAAAAAAAA</td> <td>**********AAAA</td> </tr> <tr> <td>SCRUB_CC.Solid_UNICODE</td> <td>UUUUUUUUUUUUUUUU</td> <td>**********UUUU</td> </tr> <tr> <td>SCRUB_AMEX.Solid_ANSI</td> <td>AAAAAAAAAAAAAAA</td> <td>**********AAAA</td> </tr> <tr> <td>SCRUB_AMEX.Solid_UNICODE</td> <td>UUUUUUUUUUUUUUUU</td> <td>**********UUUU</td> </tr> </tbody> </table> <p>Regex with Redact - Use of Regular expressions (regex) in the IBM® Guardium® solution (including masking in the policy) runs on the appliance, and allows advanced regex capabilities.</p> <p>However, the regex library for use with Redaction runs in the kernel of the database server and is limited to most basic regex. Only basic regex patterns can be used with Redaction.</p> <p>For example, the regular expression nomenclature [0-9]* cannot be used to indicate any number of digits. Use basic regular expression nomenclature, for example, [0-9]-[0-9]-[0-9]... to specify a sequence of digits.</p> <p>Note: S-TAP accepts only the predefined SCRUB pattern names; ignoring any other name.<br/>Access rule, data pattern, and replacement character - Using a data pattern such as <code>[a-z,2]{3}([_][0-9]{1,2})</code> with a replacement character of * changes the values between the parentheses in the data pattern to ***. Use this function to mask values.</p> <p>User-Defined Character Sets</p> <p>Available for Oracle, Sybase, MySQL, and MSSQL and for extrusion rules only, users can influence the character set used by defining special extrusion rules. These character set policy rules are only used to set the character set a user wants to convert traffic to, setting an action is irrelevant. To have an action for that traffic, the user needs to define additional rules after that character set rule. Two examples of setting a character set rule are possible (hint or force) as defined in the following examples:</p> <p>Example of extrusion rule (with hint).</p> <p>Converts the traffic by character set as defined in the extrusion rule of the installed policy ONLY if the regular conversion failed.</p> <p><b>Character set EUC-JP (code 274) .</b></p> <p>Extrusion rule pattern: <code>guardium://char_set?hint=274</code></p> <p>Example of extrusion rule (with force).</p> <p>Converts the traffic by character set as defined in the extrusion rule of the installed policy for ALL data.</p> <p><b>Character set EUC-JP (code 274) .</b></p> <p>Extrusion rule pattern: <code>guardium://char_set?force=274</code></p> <p>Note: Keep in mind that extrusion rules usually attached to the session with delay. Therefore short sessions or beginning of a session might not be immediately affected by character set change.</p> | Name :                 | Pattern: | Masked to: | SCRUB_SSN_ANSI | AAA-AA-AAAA | ****-****-AAAA | SCRUB_SSN_UNICODE | UUU-UU-UUUU | ****-****-UUUU | SCRUB_CC_SPACES_ANSI | AAAA AAAA AAAA AAAA | ***** ***** ***** AAAA | SCRUB_CC_SPACES_UNICODE | UUUU UUUU UUUU UUUU | ***** ***** ***** UUUU | SCRUB_CC.Solid_ANSI | AAAAAAAAAAAAAAA | **********AAAA | SCRUB_CC.Solid_UNICODE | UUUUUUUUUUUUUUUU | **********UUUU | SCRUB_CC_AX.Solid_ANSI | AAAAAAAAAAAAAAA | **********AAAA | SCRUB_CC_AX.Solid_UNICODE | UUUUUUUUUUUUUU | **********UUUU | Name : | Pattern: | Masked to: | SCRUB_SSN_ANSI | AAA-AA-AAAA | ****-****-AAAA | SCRUB_SSN_UNICODE | UUU-UU-UUUU | ****-****-UUUU | SCRUB_CC_SPACES_ANSI | AAAA AAAA AAAA AAAA | **********AAAA | SCRUB_CC_SPACES_UNICODE | UUUU UUUU UUUU UUUU | **********UUUU | SCRUB_CC.Solid_ANSI | AAAAAAAAAAAAAAA | **********AAAA | SCRUB_CC.Solid_UNICODE | UUUUUUUUUUUUUUUU | **********UUUU | SCRUB_AMEX.Solid_ANSI | AAAAAAAAAAAAAAA | **********AAAA | SCRUB_AMEX.Solid_UNICODE | UUUUUUUUUUUUUUUU | **********UUUU |
| Name :                    | Pattern:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Masked to:             |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |
| SCRUB_SSN_ANSI            | AAA-AA-AAAA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | ****-****-AAAA         |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |
| SCRUB_SSN_UNICODE         | UUU-UU-UUUU                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | ****-****-UUUU         |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |
| SCRUB_CC_SPACES_ANSI      | AAAA AAAA AAAA AAAA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | ***** ***** ***** AAAA |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |
| SCRUB_CC_SPACES_UNICODE   | UUUU UUUU UUUU UUUU                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | ***** ***** ***** UUUU |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |
| SCRUB_CC.Solid_ANSI       | AAAAAAAAAAAAAAA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | **********AAAA         |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |
| SCRUB_CC.Solid_UNICODE    | UUUUUUUUUUUUUUUU                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | **********UUUU         |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |
| SCRUB_CC_AX.Solid_ANSI    | AAAAAAAAAAAAAAA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | **********AAAA         |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |
| SCRUB_CC_AX.Solid_UNICODE | UUUUUUUUUUUUUU                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | **********UUUU         |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |
| Name :                    | Pattern:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Masked to:             |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |
| SCRUB_SSN_ANSI            | AAA-AA-AAAA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | ****-****-AAAA         |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |
| SCRUB_SSN_UNICODE         | UUU-UU-UUUU                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | ****-****-UUUU         |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |
| SCRUB_CC_SPACES_ANSI      | AAAA AAAA AAAA AAAA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | **********AAAA         |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |
| SCRUB_CC_SPACES_UNICODE   | UUUU UUUU UUUU UUUU                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | **********UUUU         |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |
| SCRUB_CC.Solid_ANSI       | AAAAAAAAAAAAAAA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | **********AAAA         |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |
| SCRUB_CC.Solid_UNICODE    | UUUUUUUUUUUUUUUU                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | **********UUUU         |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |
| SCRUB_AMEX.Solid_ANSI     | AAAAAAAAAAAAAAA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | **********AAAA         |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |
| SCRUB_AMEX.Solid_UNICODE  | UUUUUUUUUUUUUUUU                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | **********UUUU         |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |
| DB Name                   | The database name. For more information, see <a href="#">Values and groups of values in rules</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                        |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |
| DB Type                   | <p>Supported DB Types</p> <p>For access rule: Cassandra, CIFS, CouchDB, Db2, Db2 COLLECTION PROFILE* (only for use with z/OS), FTP, GreenPlumDB, Hadoop, HTTP, IBM INFORMIX (DRDA), IBM iSeries, IMS, IMS COLLECTION PROFILE (only for uses with z/OS, Informix®, MongoDB, MS SQL SERVER, MYSQL, NETEZZA, Oracle, PostgreSQL, Sybase, TERADATA, VSAM, or VSAM COLLECTION PROFILE* (only for use with z/OS)).</p> <p>For exception and extrusion rules: Cassandra, CIFS, CouchDB, Db2, FTP, GreenPlumDB, Hadoop, IBM INFORMIX (DRDA), IBM iSeries, Informix, MongoDB, MS SQL SERVER, MYSQL, NETEZZA, Oracle, PostgreSQL, Sybase, or TERADATA. Note: Informix supports two protocols SQLEXEC (native Informix protocol) or DRDA (IBM protocol). These protocols are automatically identified for Informix traffic with no additional settings. The Server Type attribute shows INFORMIX (for SQLEXEC protocol) and IBM INFORMIX (DRDA) (for DRDA protocol).</p> <p>Note: TERADATA has a silent login and allows clients to auto-reconnect. To block Teradata statements in a policy, use the S-TAP firewall function with default state ON and unwatch safe users.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                        |          |            |                |             |                |                   |             |                |                      |                     |                        |                         |                     |                        |                     |                 |                |                        |                  |                |                        |                 |                |                           |                |                |        |          |            |                |             |                |                   |             |                |                      |                     |                |                         |                     |                |                     |                 |                |                        |                  |                |                       |                 |                |                          |                  |                |

| Field                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DB User                    | The database user. For more information, see <a href="#">Values and groups of values in rules</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Error Code                 | The error code (for an exception). For more information, see <a href="#">Values and groups of values in rules</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Exception Type             | <p>The type of exception (selected from the list).</p> <p>SECURITY INCIDENT is an exception type generated using the session level policy actions LOG EXCEPTION or THROW EXCEPTION. In general, security incidents are detected either through manually-created policy actions or by one of the predefined security incident templates. For more information, see <a href="#">Security incident policies</a>.</p> <p>Note: A session closed by GUI timeout, in an Exception rule, does not produce a Session Error (Session_Error).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Field Name                 | <p>The field name. For more information, see <a href="#">Values and groups of values in rules</a>.</p> <p>If the Every member in group option is selected, all fields of the SQL statement must be a member of the defined group. However, the SQL statement does not need to contain all members of the group. For example, for the group <b>DB_TABLES_PROD</b> with members <b>students</b>, <b>module</b>, <b>marks</b>:</p> <ul style="list-style-type: none"> <li>For the query <code>select * from students;</code>, the object <b>students</b> is in the group and triggers the rule.</li> <li>For query <code>select * from students, module, marks;</code>, all three objects are in the group, which triggers the rule.</li> <li>For the query <code>select * from students, test;</code>, the object <b>test</b> is not in the group and does not trigger the rule when the Every member in group option is selected. However, it triggers the rule if the In group option is selected, since <b>students</b> is a member of the group.</li> </ul>                                                                                                                                                                                                                   |
| Min. Ct.                   | The minimum number of times the condition that is contained in the rule must be matched before the rule is satisfied (subject to the Reset interval).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Net. Protocol              | The network protocol. For more information, see <a href="#">Values and groups of values in rules</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Object                     | <p>The object name. For more information, see <a href="#">Values and groups of values in rules</a>.</p> <p>For Sybase and MS SQL Server, two groups MASKED_SP_EXECUTIONS_SYBASE and MASKED_SP_EXECUTIONS_MS_SQL_SERVER include names of stored procedures. If an included procedure runs, then everything is masked.</p> <p>If the Every member in group option is selected, all fields of the SQL statement must be a member of the defined group. However, the SQL statement does not need to contain all members of the group. For example, for the group <b>DB_TABLES_PROD</b> with members <b>students</b>, <b>module</b>, <b>marks</b>:</p> <ul style="list-style-type: none"> <li>For the query <code>select * from students;</code>, the object <b>students</b> is in the group and triggers the rule.</li> <li>For query <code>select * from students, module, marks;</code>, all three objects are in the group, which triggers the rule.</li> <li>For the query <code>select * from students, test;</code>, the object <b>test</b> is not in the group and does not trigger the rule when the Every member in group option is selected. However, it triggers the rule if the In group option is selected, since <b>students</b> is a member of the group.</li> </ul> |
| Object/Command Group       | Match a member of the selected Object/Command group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Object/Field Group         | Match a member of the selected Object/Field group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| OS User                    | Operating system user. For more information, see <a href="#">Values and groups of values in rules</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Pattern                    | A regular expression to be matched, in the Pattern box. You can enter a regular expression manually, or click theRegex) button to open the Build Regular Expression tool, which allows you to enter and test regular expressions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Time Period                | To make the rule sensitive to a single time period, select a pre-defined time period from the Period list or click thePeriod) button to define a new time period.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Rec. Vals.                 | When marked, the actual construct causing the rule to be satisfied will be logged, and available in reports, in the SQL String attribute. For a policy violation only, if not marked, no SQL statements will be logged.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Records Affected Threshold | <p>Access rule only. Set a threshold value for matched records. For example: Let 100 instances take place before taking action.</p> <p>This field affects the rule output rather than the rule definition (that is, what happens when it is triggered, rather than when should it trigger).</p> <p>You can select how to calculate the records affected threshold. The choices are as follows:</p> <ul style="list-style-type: none"> <li>Per session</li> <li>Per single query</li> <li>By the exceeded row count, that is, when the number of affected records exceeds the number of records that the Guardium sniffer is configured to process at one time)</li> </ul> <p>If the threshold reaches the specified number, and any other rule criteria are matched, the defined rule actions are triggered.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Replacement Character      | <p>Define a masking character.</p> <p>Should the output produced by the extrusion rule match the regular expression, the portions that match sub-expressions between parenthesis '(' and ')' will be replaced by the Masking character.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Reset Interval             | Used only if the Min. Ct. field is greater than zero. This value is the number of minutes after which the condition met counter will be reset to zero.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Response length threshold  | <p>For access rules: Tracks the size of data packets, in bytes, returned from the server for a successful SQL query. You can set the response length and the response length threshold as follows:</p> <ul style="list-style-type: none"> <li>Per session (calculates the sum of all response lengths in the session)</li> <li>Per single query (stores the response length for each SQL query)</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Revoke                     | This checkbox appears on extrusion rules only. It allows you to exclude from logging a response that has already been selected for logging by a previous rule in the policy. In most cases you can accomplish the same result more simply by defining a single rule with one or more NOT conditions to exclude the responses you do not want, while logging the remaining ones that satisfy the rule. (The Revoke checkbox pre-dates NOT conditions, and is provided mainly for backward compatibility to support existing policies.)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Field                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rule Description                   | <p>The name of the rule. To use a special pattern test in the rule, enter the special pattern test name followed by a space and one or more additional characters to make the rule name unique, for example: guardium://SSEC_NUMBER employee. (See Special Pattern Tests for more information.)</p> <p>When displayed, the name will be prefaced with the rule number and the label Access Rule, Exception Rule, or Extrusion Rule, to identify the rule type. If the rule was generated using the Suggest From DB function, the generated name is in the format: Suggested Rule &lt;n&gt;_mm-dd hh:mm, consisting of the following components</p> <p>n is sequence number for the generated rule</p> <p>mm-dd is the month and day the rule was generated</p> <p>hh:mm is the time the rule was generated</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Server IP                          | <p>Clear the Not box to include, or mark the Not box to exclude:</p> <ul style="list-style-type: none"> <li>Any server: Leave all server fields blank. The count will be incremented every time any server satisfies the rule. (You cannot leave all fields blank if the Not box is marked.)</li> <li>All servers selected by an IP address and mask: Enter a server IP address in the first box, and network mask in the second box. The count will be incremented each time that any of the specified servers satisfies the rule. For example, to select all servers in subnet 192.168.3.x, enter 192.168.3.1 in the first box, and 255.255.255.0 in the second box.</li> <li>A group of servers: Select a group of server IP addresses from the Group drop-down list or click the Groups button to define a new group and then select that group. The count will be incremented each time that any member of the specified group satisfies the rule.</li> <li>All servers selected by an IP address and mask AND a group of servers: Use both the Server IP and Group fields. The count will be incremented each time that any server specified using either method satisfies the rule.</li> </ul> <p>Allow wildcard in IP address. Wildcard % is permitted in a policy for Server IP group.</p> |
| Service Name                       | The service name. For more information, see <a href="#">Values and groups of values in rules</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Severity                           | Select a severity code from the list: INFO, LOW, NONE, MED or HIGH. If HIGH is selected and email alerts are sent by this rule, the email will be flagged Urgent.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| SQL Pattern                        | A regular expression to be matched, in the Pattern box. You can enter a regular expression manually, or click Regex  to open the Build Regular Expression tool, which allows you to enter and test regular expressions.<br>Restriction: SQL Pattern is not supported for redaction rules.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Src app                            | Application source program. For more information, see <a href="#">Values and groups of values in rules</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Trigger Once Per Session           | Do not analyze session for same rule after first match. Especially effective for "Selective Audit" policies.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| XML Pattern                        | A regular expression to be matched, in the Pattern box. You can enter a regular expression manually, or click Regex  to open the Build Regular Expression tool, which allows you to enter and test regular expressions.<br>A regular expression to be matched can be used in this box. The regular expression must be entered manually.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Full_SQL return values using MSSQL | In MSSQL, sp_cursoropen and sp_cursorfetch stored procedures are used for SELECT database queries.<br>Sp_cursoropen holds the original statement, while the FULL_SQL return value in an Extrusion rule will appear as sp_cursorfetech instead of Select * from _____.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Creating and installing a policy and policy rules

Use the Policy Builder for Data to manage policies and policy rules.

### About this task

The Policy Builder for Data provides a single solution for creating and modifying policies, policy rules, and policy rule actions. This procedure describes an end-to-end workflow for creating and installing a policy.

Note: After you update a policy (such as changes to group members, policy rules, or actions), you must reinstall the policy. You can either reinstall the policy on a managed unit, or select **Policy installation schedule** from the configuration profile. Use the **Policy installation schedule** to schedule a distribution that pushes the policy from the central manager to specified managed units. For more information, see [Working with configuration profiles](#).

Important: Policies that are installed from the central manager to an aggregator might appear in the aggregator UI as not installed because you cannot install policies on an aggregator. To determine whether a policy is installed, run the [list\\_installed\\_policies](#) API or check in the Policy Builder for Data page for each aggregator.

### Procedure

1. Navigate to Protect > Security Policies > Policy Builder for Data.
2. Create a policy or clone an existing policy or policy template.

- To create a new policy, click the  icon.
  - To clone an existing policy, select an existing policy or policy template from the Security Policies window and click the  icon.  
Tip: Guardium provides templates of predefined policies that you can use to build similar policies. Clone the [template] version and customize it as needed.
- a. From the Name and properties ribbon of the Create New Policy page, specify a policy Type and policy Name.  
Note: The policy name must not exceed 255 characters.
  - b. Optional: For data-security policies, specify additional settings.
    - Use the Category field to provide an arbitrary label for grouping policy violations for reporting purposes. The category that is specified here is used as the default category for each rule and can be overridden in individual rule definitions.
    - Click Show advanced options to work with the following settings:
      - [Log flat](#)
      - [Rules on flat](#)

- [Selective audit trail](#)
3. Click the Rules ribbon to begin working with policy rules.
- To create a new rule, click the  icon.
  - To clone a rule, select an existing rule and click the  icon.
  - To edit a rule, select an existing rule and click the  icon.
- a. From the Rule definition ribbon of the Create New Rule window, specify a Rule type and Rule name.  
 Note: The rule name must not exceed 255 characters.  
 For access and exception rules, optionally specify Category and Classification values for reporting purposes, and define the rule Severity.
- b. Click the Rule criteria ribbon and begin defining rule parameters and values.  
 Some rule criteria are only available for specific rule types or are only available after other criteria are defined. The policy builder manages these dependencies for you: criteria are available for use only in valid contexts.
- Use the menus to select individual parameters and define selection operators before you specify values or groups to match.
  - Use the  and  icons to add or remove criteria from the rule.
- For more information about rule criteria, see [Rule definition fields](#) and [Values and groups of values in rules](#).
- c. Optional: After defining criteria on the Rule criteria ribbon, select the Continue to next rule checkbox.  
 Use this setting in cases where it is necessary to take multiple actions for the same or similar conditions. For more information, see [Continue to next rule](#).
- d. Click the Rule action ribbon to begin working with rule actions.
- To create a new rule action, click the  icon and select an action. If further configuration is required, use the Add New Action window to define the action.
  - To edit a rule action, select an existing action and click the  icon and use the Edit Action window to update the rule action configuration.
- For more information about available actions, see [Policy rule actions](#).
- e. When you finish defining the rule, click OK to return to the Rules ribbon.  
 Continue creating, cloning, and editing rules as needed.
4. When you finish defining the policy and its rules, click OK to save the policy and return to the Security Policies table.

## What to do next

To install policies, select a policy from the Security Policies window and click [Install > Install](#). Select the Installation action you want and click OK to install the policy.

Installed policies are indicated by a  in the Installed column.

You can also install policies by using [Protect > Security Policies > Policy Installation](#). For more information, see [Using the Policy Installation tool](#).

Note: From Security Policies title bar, you can begin to create a IBM® Knowledge Catalog - Guardium® integration by clicking Configure WKC. For more information, see [Integrating with IBM Knowledge Catalog for federated data protection](#).

## Tagging policy rules

Guardium provides predefined policy rule tags and supports custom tagging of rules. Use tags to quickly create and manage policies aligned with specific compliance standards, reporting and auditing requirements, or geographies.

## Procedure

1. Open [Protect > Security Policies > Policy Builder for Data](#).
2. Use the  icon to create a new policy, or select an existing policy and use the  icon to edit.
3. In the Rules section of the policy builder, begin working with tags.
  - **[Importing rules by tag](#)**  
 Use one or more tags to add collections of policy rules to a policy. This includes predefined rules and tags provided by Guardium as well as custom rules and tags created for your organization. Importing rules by tags allows you to easily create policies that support your specific reporting and auditing requirements, for example by combining Guardium's predefined rules for GDPR with a set of custom rules.
  - **[Adding tags while defining policy rules](#)**  
 It is easy to add tags while creating or editing policy rules. Tagging allows you to add rules to Guardium's predefined collections or establish your own collections of rules. It's also possible to include the same rule in multiple collections by applying multiple tags.
  - **[Managing policy rule tags](#)**  
 Easily manage policy rule tags directly from the policy builder for data.

## Importing rules by tag

Use one or more tags to add collections of policy rules to a policy. This includes predefined rules and tags provided by Guardium as well as custom rules and tags created for your organization. Importing rules by tags allows you to easily create policies that support your specific reporting and auditing requirements, for example by combining Guardium's predefined rules for GDPR with a set of custom rules.

## Before you begin

Open the Policy Builder for Data and begin working with the Rules section of a specific policy.

## Procedure

1. From the Rules section of the Policy Builder for Data, click Import.

2. From the Import rules from policy dialog, select Import by tags.
3. Use the Select a tag menu to select one or more tags.
4. Optional: Use the Show only template rules check box to hide or show custom rules.
5. Use the check boxes to select the rules to import.
6. Use the Import after rule menu to define where to add the rules in the policy.
7. Click OK to import the rules into the policy.

---

## Adding tags while defining policy rules

It is easy to add tags while creating or editing policy rules. Tagging allows you to add rules to Guardium's predefined collections or establish your own collections of rules. It's also possible to include the same rule in multiple collections by applying multiple tags.

### Before you begin

Open the Policy Builder for Data and begin working with the Rules section of a specific policy.

### Procedure

1. From the Rules section of the Policy Builder for Data, use the  icon to create a new rule, or select an existing rule and use the  icon to edit.
2. From the Rule definition section, use the Tags menu to add or remove tags on the rule.
  - Use the check boxes to select to deselect tags.
  - Use the  icon to create new tags.
3. Continue working with rule definition, rule criteria, and rule action.
4. Click OK to save the rule and apply the tags.

---

## Managing policy rule tags

Easily manage policy rule tags directly from the policy builder for data.

### Before you begin

Open the Policy Builder for Data and begin working with the Rules section of a specific policy.

### Procedure

1. From the Rules section of the Policy Builder for Data, use the check boxes to select one or more rules.
2. Click Tag.
3. From the Manage tags for policy rules dialog, use the Tags menu to add or replace tags for the rules.
  - Use the menu to select an existing tag.
  - Use the  icon to create a new tag.
4. Define the tagging action.
  - Select Replace existing policy rule tags to replace all existing tags on the rules with the selected tag.
  - Select Add to existing policy rule tags to add the selected tag to the existing tags on the rules.
5. Click Save to update the tags on the rules.

---

## Using the Policy Installation tool

Learn how to install a policy on your Guardium system.

### Install a policy

1. Go to Protect > Security Policies > Policy Builder for Data to open the Security Policies page.
2. Select the policy to be installed.
3. Click Install > Install. The Install policy window opens.
4. Select an Installation action.
  - Install and override: delete all installed policies and install the selected one instead.
  - Install first: install the selected policy as the first one in the sequence (before all currently installed policies).
  - Install last: install the selected policy as the last one in the sequence (after all currently installed policies, which gives it the lowest priority).
5. Select the collectors on which to install the policy.
6. Click OK. The system responds with a message indicating success, or not.
7. Optionally, go to the Policy Installer and click Modify Schedule to open the scheduling utility, to schedule recurring installation.

### Multi-policy support

More than one installed policy is permitted at the same time. All installed policies are available for action. There are two limitations: policies defined as selective audit policies can not be mixed with policies not defined as selective audit policies, and policies defined as flat log cannot be mixed with policies not defined as flat log. If trying

to mix policies, an error message results when installing these mixed policies.

The order of appearance can be controlled during the policy installation, such as first, last, or somewhere in between. But the order of appearance can not be edited at a later date.

On the Security Policies page, click  to remove an installed policy.

The first installed policy has a special meaning, as it sets the value of the global policy parameters. These parameters are: Global pattern; Is it a selective audit; Client and Server net mask; Tagged Client and Server group ID.

This multi-policy support is available through the GUI (Setup > Tools and Views > Policy Installation) and through GuardAPI.

## View policy rules for the installed policy

---

In the Currently Installed Policies page, any user can view the rules of the installed policy, and in addition, authorized users can open the policy for editing.

1. Go to Protect > Security Policies > View Installed Policy to open the Currently Installed Policies page.
2. Click View Details Report to see a detailed list of installed policies and rules.
3. Click  to edit the policy and its rules.

## Related concepts

---

- [Scheduling](#)
- [Job dependencies](#)

## Running policy analyzer and reviewing results

---

Policy analyzer provides insights that help identify frequently fired rules, optimize rule order, and evaluate rule changes.

## Before you begin

---

Policy analyzer works with standalone Guardium systems or managed units in a centrally managed environment and requires currently installed policies to evaluate traffic.  
Note:

- The policy analyzer supports up to 128 rules across all installed policies. This restriction applies to the policy analyzer only.
- Policy analyzer does not support push-down policies from z/OS S-TAPs.

## About this task

---

There are two policy analyzer modes: continuous and ad hoc. Continuous analysis records and evaluates data at predefined intervals and is useful for observing longer-term trends in policy activity. Ad hoc analyses run once, at a time you define, and are useful for evaluating specific policy changes.

## Procedure

---

1. Begin by navigating to Protect > Security policies > Policy builder for data and clicking the Analyze menu.
2. Confirm that policy analyzer is running. If necessary, start policy analyzer by clicking the Start policy analyzer link.
3. Optional: Configure the continuous analysis interval by clicking the Change policy analyzer settings link and specifying an interval.
4. Optional: Start an ad hoc analysis by clicking the Run ad hoc analysis link.
  - a. On the Run ad hoc analysis dialog, use the Start date fields to define a date and time to begin the analysis.
  - b. Use the Duration fields to define how long to run the analysis.

Tip:

  - Use the time and duration settings to evaluate traffic before and after modifying a policy to better understand the impact of the policy change.
  - The schedules for ad hoc policy analyzer jobs are not editable and cannot overlap.
  - c. Click OK to begin the ad hoc analysis.
5. View policy analyzer results by clicking the View results link and selecting either Ad hoc analysis or Continuous analysis.  
For continuous analysis, use the Time frame setting to change how much data is displayed. For ad hoc analysis, use the Start time menu to view a specific set of ad hoc results.  

The % fired among transactions for each rule chart shows what percentage of all transactions cause each rule to fire. Because not all transactions fire a rule, the total will not always equal 100%.

The Top rules (fire count) chart shows the number of times that a rule fired during the continuous analysis period or during the ad hoc analysis. Click the chart to see a key that identifies the chart contents. Click the Top rules (fire count) label and select Change selected rules to hide or show specific rules in the chart.

The Details for all policy rules table summarizes activity for policies, rules, and rule actions.

  - Use the % fired among transactions column to see how often rules are firing, expressed as a percentage of all transactions evaluated in the specified time frame.
  - Use the % fired among rules column to see which rules are firing the most, expressed as a percentage of all rules that have fired during the specified time frame.
6. Investigate specific results.
  - a. Click a bar in the % fired among transactions chart to select the corresponding row in the Details for all policy rules table or click to select any row in the table.
  - b. Investigate the selected row by clicking Actions > Full SQL log details or Violation log details.  
The details view provides information about the specific clients, users, and programs triggering the selected policy rule.

# Security incident policies

Guardium® provides several session level policy templates that encapsulate security problems that are frequently found at run time.

Each of the security incident policies contains rules that find and report on a specific type of security incident.

Many of the rules within these policies are also used by the real-time trust evaluator policies. For more information, see [Real-time trust evaluator](#).

Note: While the security incidents policies use many of the same rules as the real-time trust evaluator, they are separate entities.

The following security incident policies trigger relevant runtime actions.

- **Security anomalies**

An anomaly is behavior by a particular source that is outside of the “normal” timeframe or scope of the particular database or user's activity. Anomaly detection can indicate a security violation, even if the activities themselves do not directly violate an existing security policy.

- **Access to unaudited sensitive data**

The **Security incidents: access to unaudited sensitive data** identifies situations where either a user accesses a table that contains sensitive data, or sensitive data is improperly labeled (for example, is not in a **Sensitive data** group).

- **Administrative user accessing sensitive data**

The **Security incidents: Administrative user accessing sensitive data** identifies situations where an unauthorized administrative user tries to access sensitive data.

- **Administrative users and applications**

The **Security incidents: administrative users and applications** template provides a number of rules that track and report on possible security incidents that might be encountered at run time. You can choose which rules you need for your security scenario.

- **All users**

The **Security Incidents: all users** template provides a number of rules that track and report on possible security incidents that might be encountered at run time. You can choose which rules you need for your security scenario.

- **Credential stuffing attack**

Credential stuffing is method of hacking a system by injecting breached username and password pairs in an attempt to fraudulently gain access to user accounts. The **Security Incidents: credential stuffing attack** policy helps identify possible credential stuffing attacks.

- **Repeated failed logins or possible denial of service attack**

The **Security Incidents: repeated failed logins or possible denial of service attack** template looks for repeated failed logins or possible denial of service attacks for both database and administrative users.

- **Suspicious user activity with sensitive data (user not privileged)**

The **Security incidents: Suspicious user activity with sensitive data (user not privileged)** policy identifies situations where an unauthorized user tries to access sensitive data.

- **Quarantine users with multiple failed logins**

12.1 and later In the multiple failed login quarantine method, users are allowed five failed login attempts before they are locked out of the system and quarantined for 30 minutes. Use the **Multiple Failed Login Quarantine[template]** to create this policy.

## Security anomalies

An anomaly is behavior by a particular source that is outside of the “normal” timeframe or scope of the particular database or user's activity. Anomaly detection can indicate a security violation, even if the activities themselves do not directly violate an existing security policy.

Each rule, except for **Server encounter first time in the audit**, sets the TRUST LEVEL score to MEAN in the **Session** report. For all rules, the messages are generated in the **Connection Exceptions** report when a suspicious activity is found.

Note: The **Connection Exceptions** report data displays in managed user environments, unless you populate the Exception table on the central manager.

In addition, anomaly detection begins after Guardium detects a sufficient number of unique connections. The number of “sufficient connections” to detect anomalies is based on your environment and set without user involvement, but it is always greater than 1000 connections.

The **Security anomalies** policy contains the following rules:

Suspicious client connection

This rule identifies when new client connects to a server. Any unknown client hostname that is encountered after Guardium® detects a sufficient number of connections is considered suspicious.

This rule generates exception messages in the **Connection Exceptions** report for each unique CLIENT\_HOST\_NAME that is identified as suspicious.

Suspicious DB user connection

The S-TAP encountered an unknown or unexpected database type. Any unknown DB user connection that is encountered after Guardium detects a sufficient number of connections is considered suspicious.

This rule generates exception messages in the **Connection Exceptions** report for each unique DB\_USER identified as suspicious.

Suspicious OS user and DB user combination connection

An unexpected combination of OS user and database user was detected. Any new combination of DB User and OS User after Guardium detects a sufficient number of connections is considered suspicious.

This rule generates exception messages in the **Connection Exceptions** report for each unique OS\_USER and DB\_USER combination that is identified as suspicious.

Suspicious OS user connection

A new OS user connected to a server. Any unknown OS user that is encountered after Guardium detects a sufficient number of connections is considered suspicious.

This rule generates exception messages in the **Connection Exceptions** report for each unique OS\_USER that is identified as suspicious.

Unexpected DB type per server IP identification

A new database user connected to a server. Any unknown database user that connects to a specific server after Guardium detects a sufficient number of connections is considered suspicious.

This rule generates exception messages in the **Connection Exceptions** report for each unique DB\_TYPE that is identified as suspicious.

Unexpected command on connection start

An unexpected command was used at the connection start. Any new command on connection start that is seen after Guardium detects a sufficient number of connections is considered suspicious.

This rule generates exception messages in the **Connection Exceptions** report for each unique command on connection start that is identified as suspicious.

Unexpected error on connection start

An unexpected error occurred at the connection start. Any new error on connection start that is seen after Guardium detects a sufficient number of connections is considered suspicious.

This rule generates exception messages in the **Connection Exceptions** report for each unique error on connection start that is identified as suspicious.

#### Unexpected client time zone

Any client connection from a new time zone that is seen after Guardium detects a sufficient number of connections is considered suspicious.

This rule generates exception messages in the **Connection Exceptions** report for each unique client time zone that is identified as suspicious.

#### Unexpected authentication type

Client connected by using an unexpected authentication type. Any new authentication type for this client that is seen after Guardium detects a sufficient number of connections is considered suspicious.

This rule generates exception messages in the **Connection Exceptions** report for each unique authentication type that is identified as suspicious.

#### Unexpected authentication type for this DB type

Unexpected authentication type used for this database. Any new authentication type for this database type that is seen after Guardium detects a sufficient number of connections is considered suspicious.

This rule generates exception messages in the **Connection Exceptions** report for each new unique authentication type for this DB type that is identified as suspicious.

#### Unexpected client OS name

A new OS client connected to a server. Any unknown client OS name that is encountered after Guardium detects a sufficient number of connections is considered suspicious.

This rule generates exception messages in the **Connection Exceptions** report for each new unique Client OS name that is identified as suspicious.

#### Server encounter first time in the audit

An unknown S-TAP is found for this server IP address. The first time a previously unseen server connects is considered an anomaly.

This rule generates exception messages in the **Connection Exceptions** report each time that a new server is identified. In addition, this rule sets the TRUST LEVEL score to 0.7 in the **Session** report.

---

## Access to unaudited sensitive data

### The **Security incidents: access to unaudited sensitive data**

This identifies situations where either a user accesses a table that contains sensitive data, or sensitive data is improperly labeled (for example, is not in a **Sensitive data** group).

#### The **Security incidents: access to unaudited sensitive data** contains the following rules:

##### Configure server data to detect sensitive data exfiltration

This rule configures the server to detect when an unauthorized user accesses a table that contains sensitive data.

##### Identify sensitive data that has not been previously audited

This rule identifies sensitive data (in this case, credit card data) that is not properly labeled as sensitive.

##### Generate a security incident exception

This rule generates an exception message in the **Security Incident** report when an unauthorized database user attempts to access the sensitive data.

---

## Administrative user accessing sensitive data

### The **Security incidents: Administrative user accessing sensitive data**

This identifies situations where an unauthorized administrative user tries to access sensitive data.

#### The **Security incidents: Administrative user accessing sensitive data** contains the following rules:

##### Identify access to sensitive data by administrative user

This rule configures the server to detect when an unauthorized administrative user accesses a table that contains sensitive data.

##### Generate security incident

This rule generates an exception message in the **Security Incident** report when an unauthorized administrative user attempts to access the sensitive data.

---

## Administrative users and applications

### The **Security incidents: administrative users and applications**

This template provides a number of rules that track and report on possible security incidents that might be encountered at run time. You can choose which rules you need for your security scenario.

Some rule definitions are tagged as either PCI or GDPR. These tags indicate that the rule can help meet compliance with either payment card information (PCI) or General Data Protection Regulation (GDPR) rules.

By default, each rule includes the MARK SESSION action, which sets the trust for this session to LOW and generates an exception in the Security Incidents report.

Note: The security incident policies analyze authentication methods, but do not log or analyze passwords.

#### The **Security incidents: administrative users and applications** contains the following rules:

##### Admin user using plain text password

This rule identifies when plain-text passwords are used in the authentication process for admin users. Any connection to a database that uses a driver or a database that allows sending a password in clear text over the network generates a security incident.

This rule generates exception messages in the **Security Incident** report for each unique DB\_USER and SERVER\_IP.

Prerequisite: Admin users group.

##### Administrative program using plain text password

This rule identifies when plain-text passwords are used in the authentication process for applications and programs. Any program or application that allows sending a password in clear text over the network generates a security incident.

This rule generates exception messages in the **Security Incident** report for each unique CLIENT\_IP and SOURCE\_PROGRAM.

Prerequisite: Admin programs group.

#### Unencrypted administrative session

This rule checks that the session is not encrypted and the user is part of the administrative group. This rule generates a security incident for unencrypted administrative sessions.

This rule generates exception messages in the **Security Incident** report for each unique CLIENT\_IP, DB\_USER, and SOURCE\_PROGRAM.

Prerequisite: Admin users group.

#### Unencrypted administrative program

This rule checks that the session is not encrypted and the program is part of the administrative group. This rule generates a security incident only for unencrypted administrative programs, rather than the entire session.

This rule generates exception messages in the **Security Incident** report for each unique CLIENT\_IP and SOURCE\_PROGRAM.

Prerequisite: Admin programs group.

#### Suspicious administrative activity

This rule finds and reports on users with administrative privileges who connect to a database, but either do not have administrative privileges or are not members of the administrative group. These activities can indicate an intrusion into the database.

This rule generates a security incident when a user might have inappropriate admin privileges.

This rule generates exception messages in the **Security Incident** report for each unique DB\_USER, SOURCE\_PROGRAM, and SERVER\_IP.

Prerequisite: Admin users group.

#### Suspicious administrative program activity

This rule generates a security incident when it finds connections to a database by a program that has administrative privileges, but either the program does not have administrative privileges or it was not accounted for in the administrative group. These activities can indicate an intrusion into the database.

Prerequisite: Admin programs group

#### Repeated failed login per server IP and admin user (5 in 3 minutes)

Repeated failed log-ins by an admin user (specified as five logins within 3 minutes) generate a security incident.

Note: This rule is similar to the **User Activity Monitoring** policy *Failed Login - Alert if repeated* rule. However, the rule triggers only when a user unsuccessfully attempts to log on to the same server five times within 3 minutes (rather than logging in to multiple servers within 5 minutes).

This rule generates exception messages in the **Security Incident** report for each unique DB\_USER and SERVER\_IP.

Prerequisite: Admin users group.

#### Password sent using vulnerable encryption method for admin user

Guardium® generates a security incident when passwords are sent using insufficiently secure methods. For example, when a database uses a driver with outdated encryption methods or a database sends passwords that use outdated or vulnerable encryption methods over the network.

This rule generates exception messages in the **Security Incident** report for each unique DB\_USER, CLIENT\_IP, and SOURCE\_PROGRAM.

Prerequisite: Admin users group.

#### Repeated login failures from same Program and different Admin DB users per period of time (5 in 3 minutes)

Repeated failed log-ins by an admin user (specified as five log ins within 3 minutes) generate a security incident.

Note: This rule is similar to the **User Activity Monitoring** policy *Failed Login - Alert if repeated* rule. However, the rule triggers only when a user unsuccessfully logs on to the same server five times within 3 minutes (rather than logging in to multiple servers within 5 minutes).

This rule generates exception messages in the **Security Incident** report for each unique DB\_USER and SERVER\_IP.

Prerequisite: Admin users group.

#### Admin users re-using passwords

Reusing passwords across multiple sites poses serious security risks. If an attacker can steal credentials and gain access to one account, they can also log in to any other account that uses the same password.

This rule generates exception messages in the **Security Incident** report when at two or more DB\_USERS use identical passwords.

Prerequisite: Admin users group.

#### Failed login for admin user re-using passwords

This rule generates exception messages in the **Security Incident** report when two identical or similar passwords are found for different DB\_USER login failures on the same server.

Prerequisite: Admin users group.

---

## All users

The **Security Incidents: all users** template provides a number of rules that track and report on possible security incidents that might be encountered at run time. You can choose which rules you need for your security scenario.

Some rule definitions are tagged as either PCI or GDPR. These tags indicate that the rule can help meet compliance with either payment card information (PCI) or General Data Protection Regulation (GDPR) rules.

Many rules include the MARK SESSION action, which sets the trust for this session to LOW and generates an exception in the Security Incidents report.

Note: The security incident policies analyze authentication methods, but do not log or analyze passwords.

The **Security Incidents: all users** contains the following rules:

#### DB user using plain text password

This rule identifies when plain-text passwords are used in the authentication process for database users. Any connection to a database that uses a driver or a database that allows sending a password in clear text over the network generates a security incident.

This rule generates exception messages in the **Security Incident** report for each unique DB\_USER and SERVER\_IP.

#### Password spraying attack detection

This rule identifies when an attacker attempts to gain unauthorized access to user accounts or systems by systematically trying commonly used passwords or a small set of passwords against multiple user accounts. This rule generates an exception message when more than 10 connection attempts are made by different users with the same password.

#### Source application using plain text password

This rule identifies when plain-text passwords are used in the authentication process for applications and programs. Any program or application that allows sending a password in clear text over the network generates a security incident.

This rule generates exception messages in the **Security Incident** report for each unique CLIENT\_IP and SOURCE\_PROGRAM.

#### Repeated failed login per server IP and user (5 in 3 minutes)

This rule generates a security incident for repeated failed log-ins.

Note: This rule is similar to the **User Activity Monitoring** policy *Failed Login - Alert if repeated* rule. However, the rule triggers only when a user unsuccessfully attempts to log on to the same server five times within 3 minutes (rather than logging in to multiple servers within 5 minutes).

This rule generates exception messages in the report for each unique DB\_USER and SERVER\_IP.

Repeated login failures from same Program and different DB users per period of time (5 in 3 minutes)

Repeated failed log-ins by a database user (specified as five log-ins within 3 minutes) generates a security incident.

Note: This rule is similar to the **User Activity**

**Monitoring** policy *Failed Login - Alert if repeated* rule. However, the rule triggers only when a user unsuccessfully logs on to the same server five times within 3 minutes (rather than logging in to multiple servers within 5 minutes).

This rule generates exception messages in the **Security Incident** report for each unique DB\_USER and SERVER\_IP.

Data exfiltration setup

Data exfiltration that exceeds a defined threshold during a session or in a session generates a security incident. This rule sets the thresholds for session and response exfiltration. In the CONFIGURE rule action, define the thresholds for SESSION, RESPONSE, or both.

Prerequisite: The *Session Data Exfiltration* or *Response Data Exfiltration* rules must be installed.

Session data exfiltration

This rule identifies data exfiltration by monitoring the amount of information that is extracted from the database during a single session.

This rule generates the following exception message in the **Security Incident** report when the data exfiltration threshold is reached:

**SESSION DATA EXFILTRATION: DATA EXCEEDED (SESSION\_EXFILTRATION\_LIMIT)**.

Prerequisite: The data exfiltration threshold for SESSION is defined by the *Data exfiltration setup* rule.

Response data exfiltration

This rule identifies data exfiltration by monitoring the amount of information that is extracted from the database from a specified response.

This rule generates the following exception message in the **Security Incident** report when the data exfiltration threshold for a response is reached:

**RESPONSE DATA EXFILTRATION: DATA EXCEEDED (RESPONSE\_EXFILTRATION\_LIMIT)**.

Prerequisite: The data exfiltration threshold is defined by the *Data exfiltration setup* rule.

## Credential stuffing attack

Credential stuffing is method of hacking a system by injecting breached username and password pairs in an attempt to fraudulently gain access to user accounts. The **Security Incidents: credential stuffing attack** policy helps identify possible credential stuffing attacks.

The **Security Incidents: credential stuffing attack** contains the following rules:

Prerequisite - Configure credential stuffing attack detection

This rule configures the credential stuffing attack detection.

Prerequisite: Server IP address in the Production Server group must be populated. By default, group is set to %.

Note: If you populate the group your own environment info, remove the % from the production server IP groups.

Credential stuffing attack detection

This rule detects credentials stuffing attacks and if an attack is found, the rule generates a security incident.

This rule generates exception messages in the **Security Incident** report when the number of login failures within the overall number of monitored sessions reaches a calculated threshold.

## Repeated failed logins or possible denial of service attack

The **Security Incidents: repeated failed logins or possible denial of service attack** template looks for repeated failed logins or possible denial of service attacks for both database and administrative users.

Many rules include the MARK SESSION action, which sets the trust for this session to LOW and generates an exception in the Security Incidents report.

Note: The security incident policies analyze authentication methods, but do not log or analyze passwords.

The **Security Incidents: repeated failed logins or possible denial of service attack** template contains the following rules:

Populate analyzed client IP if both client IP and analyzed client IP are empty

This rule uses a TRANSFORM action to move the IP address from HOST NAME to ANALYZED\_CLIENT\_IP.

Populate analyzed client IP if both client IP and analyzed client IP are empty and session identified as local

This rule uses a TRANSFORM action to move the IP address from SERVER IP to ANALYZED\_CLIENT\_IP.

Repeated failed login per Actual client IP and user (5 in 3 minutes)

This rule generates a security incident for repeated failed log-ins.

This rule generates exception messages in the **Security Incident** report for each unique DB\_USER and ACTUAL\_CLIENT\_IP.

Possible denial of service attack (20 in 1 minute)

A shared machine used as a client for multiple users can indicate a denial of service (DOS) attack and generates a security incident.

This rule requires that the populate rules (*Populate ANALYZED\_CLIENT\_IP if both CLIENT\_IP and ANALYZED\_CLIENT\_IP are empty* and *Populate ANALYZED\_CLIENT\_IP if both CLIENT\_IP and ANALYZED\_CLIENT\_IP are empty and session identified as local*) are also installed.

This rule generates exception messages in the **Security Incident** report when 20 DB\_USERS connect from a single ACTUAL\_CLIENT\_IP to a single SERVER\_IP within a 1-minute period.

Possible admin user denial of service attack (20 in 1 minute)

A shared machine used as a client for multiple users can indicate a denial of service (DOS) attack and generates a security incident.

This rule requires that the populate rules (*Populate ANALYZED\_CLIENT\_IP if both CLIENT\_IP and ANALYZED\_CLIENT\_IP are empty* and *Populate ANALYZED\_CLIENT\_IP if both CLIENT\_IP and ANALYZED\_CLIENT\_IP are empty and session identified as local*) are also installed.

This rule generates exception messages in the **Security Incident** report when 20 DB\_USERS connect from a single ACTUAL\_CLIENT\_IP to a single SERVER\_IP within a 1-minute period.

Prerequisite: Admin users group.

## Suspicious user activity with sensitive data (user not privileged)

The **Security incidents: Suspicious user activity with sensitive data (user not privileged)** policy identifies situations where an unauthorized user tries to access sensitive data.

The **Security incidents: Suspicious user activity with sensitive data** policy contains the following rules:

Identify access to sensitive data by unauthorized user

This rule configures the server to detect when an unauthorized user accesses a table that contains sensitive data.

Generate security incident exception

This rule generates an exception message in the **Security Incident** report when an unauthorized database user attempts to access the sensitive data.

## Quarantine users with multiple failed logins

12.1 and later In the multiple failed login quarantine method, users are allowed five failed login attempts before they are locked out of the system and quarantined for 30 minutes. Use the **Multiple Failed Login Quarantine [template]** to create this policy.

The **Multiple Failed Login Quarantine** policy contains the following rules:

Identify Multiple Failed Login

This rule identifies the users to quarantine due to multiple login failures.

Quarantine previously failed login connections

This rule uses the S-GATE SESSOIN TERMINATE action to enforce the quarantine policy and end the login session. Multiple failed logins are violation of the Payment Card Industry (PCI) data security compliance.

Tip: Ensure to populate production server group members for this policy to work as expected.

## Managing correlation alerts

An alert is a message that indicates that an exception or policy rule violation was detected. Create and manage correlation alerts from the Add Alert page.

Alerts are triggered in two ways:

- A *correlation alert* is triggered by a query that looks back over a specified time period to determine whether the alert threshold is met. The Guardium anomaly detection engine runs correlation queries on a scheduled basis. By default, correlation alerts do not log policy violations, but they can be configured to do that.
- A *real-time alert* is triggered by a security policy rule. The Guardium inspection engine component runs the security policy as it collects and analyzes database traffic in real time. For more information about real-time alerts, see [Understanding policies](#) and [Alerting rule actions](#).

Regardless of how they are triggered, Guardium logs all alerts the same way: the alert information is logged in the Guardium internal database. The amount and type of information that is logged depends on the specific alert type. The Guardium Alerter component, which also runs on a scheduled basis, processes each new alert, passing the logged information for each alert to any combination of the following notification mechanisms:

- MAIL - A Guardium user role email (User), or an external email (Email).  
When MAIL is selected, you can now tick the checkbox for Attach alert reports as CSV. Select User or Email. If Email is selected proceed to type in receivers email address. Otherwise if User is selected a user menu is displayed, choose wanted user.  
Select Save to add a receiver, or Back to exit Alert Receiver Selection window.
- SNMP - The SNMP (network information and control) server. When SNMP is selected for an Alert Notification, the Alerter passes all alert messages of that type to the single trap community for which the Alerter was configured.
- Syslog - The alert is written to syslog on the Guardium appliance (which might be configured by the Guardium Administrator to write syslog messages to a remote system).  
Note: For SNMP or SYSLOG, the maximum message length is 3000 characters. Any messages longer than that are truncated.
- Custom - A user written Java™ class to handle alerts. The Alerter passes an alert message and timestamp to the custom alerting class. You can have multiple custom alerting classes, and one custom alerting class can be an extension of another custom alerting class.
- Ticket - An external ticketing service

Note: Alerts definition and notification are not subject to Data Level Security for the following reasons,

- Alerts are not evaluated in the context of user.
- The alert might be related to databases that are associated with multiple users.
- To avoid situations where no one gets the alert notification.

Note: If an alert uses a query that contains 30 or more fields (including counters) the anomaly detection fails with an `Array out of bound exception` error message. Queries with 30 columns (or more) cannot be used for alerts. Such queries do not appear in the list of available queries for threshold alerts.

## Alerting tasks for administrators

Guardium administrators perform the following tasks:

- Customize the alert message template from the global profile.
- Configure and start thealerter, which delivers messages to SMTP, SNMP, Syslog, or custom alerting classes.
- Start and stop the anomaly detection engine, which runs the correlation alerts according to the schedules defined.

- Upload custom alerting classes to the Guardium system.

## Alerting tasks for users

---

Guardium users (and administrators) can perform the following tasks for correlation alerts,

- Define queries that can be used for correlation alerts.
- Define correlation alerts.
- Write custom alerting classes.

## Creating a correlation alert

---

A correlation alert is based on a query in any of the reporting domains. The query must be defined before you can define the alert. The query must contain at least one date field to be available to a correlation alert.

1. Click Protect->Database Intrusion Detection->Alert Builder to open the Alert Finder.
2. Click New in the Alerts Finder page to open the Add Alert page.
3. Under Settings, enter the following information
  - Name - Enter a unique name for the alert. Do not include apostrophe characters in the alert name.
  - Description - Enter a short sentence that describes the alert.
  - Category - Enter an optional category.
  - Classification - Enter an optional classification.
  - For Recommended Action, add free text as the recommended action for the specific alert.
  - Message Template - As with real-time alerts, you can choose a template for the message that is sent in case the threshold alert fires. The template uses a predefined list of variables that are replaced with the appropriate value for the specific alert. For more information about the message template, see [The alert message template](#).
  - Severity - Select a severity level from the Severity list. For an email alert, if the alert is set to HIGH, then the email is also flagged as HIGH. For more information on how severity affects syslog facility and priority, see [Facility and priority of syslog messages](#).
  - Run Frequency - Enter the number of minutes between runs of the query.
  - Select Active to activate the alert, or clear the box to save the alert definition without starting it running (it can be activated later). In a central manager environment, the alert is activated (or stopped) on all managed units when this box is marked (or cleared). To disable the alert on a specific appliance in a central manager environment, use the Anomaly Detection page of the Administrator Console.
  - Select Log Policy Violation to log a policy violation when this alert is triggered. By default, correlation alerts are logged in the Alert Tracking domain only. By marking this box, correlation alerts and real-time alerts (issued by the data access security policy) can be viewed together, in the Policy Violations domain.
  - Select View in deployment health dashboard if you want to include this alert in the deployment health dashboard.
4. Under Alert Definition, enter the following information.
  - Query - Select the query to run for this alert. The list of queries that are displayed includes all queries that meet the following criteria,
    - Contain at least one date field (timestamp).
    - Contain a Count field.
    - Can be accessed by your Guardium user account.

If the selected query contains runtime parameters, a Query Parameters window displays in the Alert Definition page. Supply appropriate parameter values for your application.

### Troubleshooting tips

- If a custom query was created in the Query-Report Builder, but the query does not appear in the Query list, then make sure that the custom query has a timestamp (date field).
- If you select a query from the Query list that needs editing, but you cannot edit the query, go to the Query-Report Builder to make the changes you need.
- Accumulation Interval - Enter the length of the time interval (in minutes) that the query examines the audit repository, counting back from the current time (for example, enter 10 to examine the last 10 minutes of data).
- Move interval window earlier by - GBDI data is not available immediately. Use this field to move the accumulation interval backwards in time, in minutes, so that the entire time interval of your query has data. Usually 120 minutes is sufficient.  
Note: Alerts that run on aggregators are based only on data within the defined merge period.
- Select Log Full Query Results to have the full report logged with the alert.
- Column - If the selected query contains one or more columns of numeric data, select a column to use for the test. The default is the last column for the query, which is always the count of occurrences aggregated in that row.
- 5. Under Alert Threshold, define the threshold at which a correlation alert is to be generated, as follows:
  - Threshold - Enter a threshold number that applies as described by the remaining fields in the window.
  - Alert condition - Select an operator that indicates how the report value relates to the threshold to produce an alert. Choose from > (greater than), >= (greater than or equal to), <= (less than or equal to), or < (less than).
  - Threshold Evaluated - Select per report if the threshold number applies to a report total, Select per line if the threshold applies to a single line of the report (the report contains the output of the selected query, which looks back over the specified accumulation time).
- If there is no data during the specified Accumulation Interval:
  - If the threshold is per report, the value for that interval is 0 (zero), and an alert is generated if the threshold condition is met. For example, if the condition specified is "Alert when value is < 1".
  - If the threshold is per line, no alert is generated, regardless of the specified condition (because there are no lines of output).
- Threshold Used - Select As absolute limit to indicate that the threshold entered is an absolute number. Select As a percentage change within period to indicate that the threshold represents a percentage of change within the time period that you select in From and To.
- As percentage change within period for the same Accumulation Period on a relative time - One relative date is entered and the alert runs the query for the current period and for the relative period (using the same interval), and checks the values as a percentage of the base period value.  
Note: If you use a relative period, each time the alert is checked it runs the query twice; once for the current period and once for the relative period.
- 6. Notification Frequency - Indicate how often (in minutes) to notify alert receivers when the alert condition is satisfied.
- 7. Under Managed Units, you can assign or exclude correlation alerts to individual managed units or managed unit groups from the central manager.
 

Under Select Units, select the managed units that you want to include for this alert,

  - This Central Manager - By default, the central manager receives alerts. Clear the checkbox to exclude the central manager.
  - All - Send alerts to all managed units.
  - Single Unit - Send alerts to the specified unit only.
  - Exclude Single Unit - Send alerts to all managed units except for the specified unit.

- Managed Unit Group - Click Select Group to select a managed unit group (or create a new group). Send alerts to all units in the specified managed unit group.
  - Exclude Managed Unit Group - Click Select Group to select a managed unit group (or create a new group). Send alerts to all managed units except for the units specified in this group.
8. Under Alert Receivers, you can optionally designate one or more persons or groups to notify when this alert condition is satisfied. To add a receiver, click Add Receiver to open the Alert Receiver Selection page.  
 Note: If the receiver of an alert is the admin user, then admin must have an assigned email address for the alert to fire.  
 Note: An additional receiver for threshold alerts is Owner (the owner/s of the database). If the query associated with the alert contains Server IP and Service name and if the alert is evaluated Per Row, then the receiver can be Owner. The Alert Notification must have: Alert Notification Type: Mail, Alert User ID: 0, Alert Destination: Owner. For more information, see [Alerting rule actions](#).
9. Optionally click Add Comments to add comments to the definition or click Roles to assign roles for the alert.  
 10. Click Apply and then Done to save your alert.

## Modifying a correlation alert

---

1. Click Protect > Database Intrusion Detection > Alert Builder to open the Alert Finder.
2. Select the correlation alert that you want to modify in the Alert Finder page.
3. Click Modify to open the Modify Alert window.
4. Modify the alert definition as needed.
5. Click Apply.

## Removing a correlation alert

---

1. Click Protect > Database Intrusion Detection > Alert Builder to open the Alert Finder.
2. Select the correlation alert that you want to remove in the Alerts Finder window.
3. Click Delete. You are prompted to confirm the action.

## Incident Management

---

The Integrated Incident Management (IIM) application provides a business-user interface with workflow automation for tracking and resolving database security incidents.

It simplifies incident management by allowing administrators to group a series of related policy violations into a single incident and assign them to specific individuals. This reduces the number of separate policy violations that oversight teams need to review.

Incident generation processes can be defined and scheduled to read the policy violations log and generate new incidents. From an incident generation process, each selected incident is:

- Assigned a unique incident number
- Assigned to a user
- Assigned a severity code
- Assigned to a category

In addition, policy violations can be assigned manually (by authorized users) to new incidents or existing incidents from the Policy Violations / Incident Management report.

Once an incident has been generated, administrators and other users work with incidents from the Incident Management tab, which is included on both the admin and user portals. From there, all other tasks can be performed (assign incidents, send notifications, assign status, and so forth).

The Incident Management functions can be accessed from the drill-down menus of the Incident Management reports. Each user may only have a subset of reports or functions available, depending on the security roles assigned to the user account.

You can create your own copies of the Incident Management reports, but those copies will not have all of the capabilities available from the pre-configured reports on the Incident Management tab. To assign incidents, severity codes, and so forth, use the reports on the Incident Management tab.

## Define an Incident Generation Process

---

An incident generation process executes a query against the policy violations log and generates incidents based on that query. Only the first 5,000 violations are included with an incident. When there are more than 5,000 violations, a new incident is created each time the process runs, and that incident includes the next 5,000 violations. By default, the definition and scheduling of incident generation processes is restricted to users with the admin role.

1. Click Comply > Tools and Views > Incident Generation to open Incident Generation Processes.
2. Click Add Process to open the Edit Incident Generation Process panel.
3. Select a query from the Query list. There are several restrictions that apply to queries used in an incident generation process. We suggest that you open the query in the Query-Report Builder to verify that it satisfies the following criteria:
  - The query must be from the Policy Violations domain.
  - The query must have the Count check box checked. See [Selecting the column display](#) for more information.
  - The main entity for the query must be the Policy Rule Violation entity.
  - The query fields for the query must not include a SQL string (from either the SQL entity or the Full SQL String attribute of the Policy Rule Violation entity).
4. Select a Severity for the incident (defaults to Info).
5. Optionally enter a Category for the incident (defaults to none).
6. Optionally enter a Threshold for generating the incident. The default is one, meaning every row returned by the query will generate an incident.
7. From the Assign to User list, select the user to whom the incident will be assigned.
8. Enter the From and To Dates for the query. For a scheduled query, use relative dates (for example: now -1 day and now).
9. Click Save to save the process definition. You cannot run or schedule the process until it has been saved.
10. To run the query now, click Run Once Now.
11. To schedule the query, click Modify Schedule to open the general-purpose scheduling utility.

## Assign/Reassign to Incident

---

1. Double-click the policy violation to be assigned or reassigned, in one of the Incident Management reports.
2. Select Assign/Reassign to incident from the drill-down menu. When selected, this menu will be replaced by a new menu containing a list of open incidents (for example, Assign to Incident #123), and one additional option: Assign to a new incident.
3. Select an incident to assign this violation to, or select Assign to a new incident to assign this Policy Violation to the next incident number available (they are numbered in sequence).  
A message is displayed when the change has been completed, and the Incident Management panel will be refreshed. If a new incident has been created, it will be listed first in the Open Incidents report.

## Assign to User

---

1. Double-click the incident to be assigned to another user, in one of the Incident Management reports.
2. Select Assign to user from the drill-down menu. When selected, this menu will be replaced by a new menu containing a list of users, and one additional option: Unassign.
3. Select a user, or select Unassign to remove the current user assigned. When a user is assigned, the Status Description will be Assigned, and when unassigned the Status Description will be Open.  
A message is displayed when the change has been completed, and the Incident Management panel will be refreshed.

## Change Severity

---

1. Double-click the incident on which the severity is to be changed, in one of the Incident Management reports.
2. Select Change Severity from the drill-down menu. When selected, this menu will be replaced by a new menu containing a list of severity codes: Info, Low, Med, and High.
3. Select the new severity code.  
A message is displayed when the change has been completed, and the Incident Management panel will be refreshed.

## Notify

---

1. Double-click the incident a user is to be notified about, in one of the Incident Management reports.
2. Select Notify from the drill-down menu. When selected, this menu will be replaced by a new menu containing a list of users.
3. Select a user.  
A message is displayed when the user has been a notification.

## Change Status

---

1. Double-click the incident on which the status is to be changed, in one of the Incident Management reports.
2. Select Change Status from the drill-down menu. When selected, this menu will be replaced by a new menu containing a list of status codes:
  - ASSIGNED - Once an incident has this status, it cannot have additional policy violations added to it. To add policy violations, change the incident status back to Open, add the violations, and then change the status back to Assigned.
  - CLOSED - Once an incident is marked Closed it cannot be modified, and is no longer listed.
  - OPEN - This is the initial status for a new incident.
3. Select the new status code.  
A message is displayed when the change has been completed, and the Incident Management panel will be refreshed.

## Add Comments

---

1. Double-click the incident to which comments are to be added, in one of the Incident Management reports.
2. Select Comments from the drill-down menu, to open the User Comment window. For instructions on how to add comments, see [Comments](#).

## How to manage the review of multiple database security incidents

---

Incident management - track and resolve database security incidents.

### About this task

---

Administrators can group a series of related policy violations into a single incident and assign to specific individuals. This reduces the number of separate policy violations that oversight teams need to review.

#### Prerequisites

- Create a Policy (See Policies).
- Start inspection engines (See Inspection Engine Configuration).

A security policy contains an ordered set of rules to be applied to the observed traffic between database clients and servers.

A policy violation is logged each time that a rule is triggered. Policy violations can be assigned to incidents, either automatically by a process, or manually by authorized users (see Incident Management).

#### Summary of Steps

1. Click Comply > Tools and Views > Incident Generation to open Incident Generation Processes.
2. Edit Incident Generation Process (Query, Severity, Threshold, Scheduling).
3. Go to Incident Management tab for reports.

## Incident Management

The Incident Management application provides a business-user interface with workflow automation for tracking and resolving database security incidents.

Incident generation processes can be defined and scheduled to read the policy violations log and generate new incidents. From an incident generation process, each selected incident is:

- Assigned a unique incident number.
- Assigned to a user.
- Assigned a severity code.
- Assigned to a category.

In addition, policy violations can be assigned manually (by authorized users) to new incidents or existing incidents from the Policy Violations / Incident Management report.

Once an incident has been generated, administrators and other users work with incidents from the Incident Management tab, which is included on both the admin and user portals. From there, all other tasks can be performed (assign incidents, send notifications, assign status, and so forth).

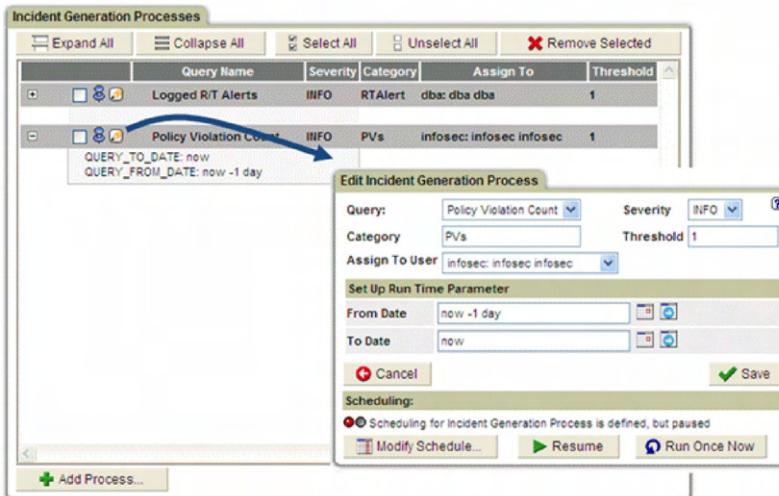
The Incident Management functions can be accessed from the drill-down menus of the Incident Management reports. Each user may only have a subset of reports or functions available, depending on the security roles assigned to the user account.

### Define an Incident Generation Process

An incident generation process executes a query against the policy violations log, and generates incidents based on that query. By default, the definition and scheduling of incident generation processes is restricted to users with the admin role.

## Procedure

- Click Comply > Tools and Views > Incident Generation to open Incident Generation Processes.
- Click the Add Process button to open the Edit Incident Generation Process panel.
- Select a query from the Query list. There are several restrictions that apply to queries used in an incident generation process. Open the query in the Query-Report Builder to verify that it satisfies the following criteria:
  - The query must be from the Policy Violations domain.
  - The query must have the Count check box checked. See [Selecting the column display](#) for more information.
  - The main entity for the query must be the Policy Rule Violation entity.
  - The query fields for the query must not include a SQL string (from either the SQL entity or the Full SQL String attribute of the Policy Rule Violation entity).
- Select a Severity for the incident (defaults to Info).
- Optionally enter a Category for the incident (defaults to none).
- Optionally enter a Threshold for generating the incident. The default is one, meaning every "row" returned by the query will generate an incident.
- From the Assign to User list, select the user to whom the incident will be assigned.
- Enter the From and To Dates for the query. For a scheduled query, use relative dates (for example: now -1 day and now).
- Click Save to save the process definition. You cannot run or schedule the process until it has been saved.
- To run the query now, click Run Once Now.
- To schedule the query, click Modify Schedule to open the scheduling utility. For instructions on how to use the scheduler, see Scheduling.



- Assign/Reassign to Incident - Double-click on the policy violation to be assigned or reassigned, in one of the Incident Management reports.
- Select Assign/Reassign to Incident from the drill-down menu. When selected, this menu will be replaced by a new menu containing a list of open incidents (for example, Assign to Incident #123), and one additional option: Assign to a new incident.
- Select an incident to assign this violation to, or select Assign to a new incident to assign this Policy Violation to the next incident number available (they are numbered in sequence). A message displays when the change has been completed, and the Incident Management panel will be refreshed. If a new incident has been created, it will be listed first on the Open Incidents report.

From the Incident Policy Violations / Incident Management report, users can:

- Assign/Reassign to Incident (create an incident from this policy violation).
- Change the severity of the incident.
- Notify one or more users about the incident.
- View reports of Client IP Activity, User Activity, or SQL from the incident.

| Violation Log Id | Timestamp           | Category Name                    | Access Rule Description | Client IP      | Server IP    | DB User Name | Full SQL String                 | Severity Description | Incident Number | Count of Policy Rule Violations |
|------------------|---------------------|----------------------------------|-------------------------|----------------|--------------|--------------|---------------------------------|----------------------|-----------------|---------------------------------|
| 52               | 2007-05-01 15:39:11 | Alert when abdiel accesses robin |                         | 192.168.20.204 | 192.168.2.45 | SA           | select @@trancount              | INFO                 | 0               | 1                               |
| 51               |                     | Assign/Reassign to Incident...   |                         |                |              |              | select * from guardium_borrower | HIGH                 | 1               | 1                               |
| 50               |                     | Change Severity...               |                         |                |              |              | select * from guardium_borrower | HIGH                 | 2               | 1                               |
| 45               |                     | Notify...                        |                         |                |              |              | set showplan_text off           | INFO                 | 0               | 1                               |
| 46               |                     | Client IP Activity Summary       |                         |                |              |              | set noexec off                  | INFO                 | 3               | 1                               |
|                  |                     | User Activity Summary            |                         |                |              |              |                                 |                      |                 |                                 |
|                  |                     | Show SQL                         |                         |                |              |              |                                 |                      |                 |                                 |

15. Assign to User - Double-click on the incident to be assigned to another user, in one of the Incident Management reports.
16. Select Assign to user from the drill-down menu. When selected, this menu will be replaced by a new menu containing a list of users, and one additional option: Unassign.
17. Select a user, or select Unassign to remove the current user assigned. When a user is assigned, the Status Description will be Assigned, and when unassigned the Status Description will be Open.
- A message displays when the change has been completed, and the Incident Management panel will be refreshed.
18. Change Severity - Double-click on the incident on which the severity is to be changed, in one of the Incident Management reports.
19. Select Change Severity from the drill-down menu. When selected, this menu will be replaced by a new menu containing a list of severity codes: Info, Low, Med, and High.
20. Select the desired severity code.

A message displays when the change has been completed, and the Incident Management panel will be refreshed.

Once a policy violation has been assigned to an incident the incident displays in the Open Incidents report. From the Open Incidents report, users can perform the actions shown:

| Open Incidents / Incident Management                          |                     |          |               |                    |            |           |               |       |                        |  |
|---------------------------------------------------------------|---------------------|----------|---------------|--------------------|------------|-----------|---------------|-------|------------------------|--|
| Start Date: 2007-04-26 09:31:57 End Date: 2007-05-04 09:31:57 |                     |          |               |                    |            |           |               |       |                        |  |
| Incident Number                                               | Timestamp           | Severity | Category Name | Status Description | First Name | Last Name | # of Comments | Count |                        |  |
| 3                                                             | 2007-05-01 14:16:44 | INFO     |               | OPEN               |            |           |               |       | Records: 1 To 2 From 2 |  |
| 2                                                             | 2007-05-01 14:18:30 | HIGH     |               | OPEN               |            |           |               |       |                        |  |

Assign to user...  
 Change Severity...  
 Notify...  
 Change status...  
 Comments...  
 Violations per incident

21. Notify - Double-click on the incident a user is to be notified about, in one of the Incident Management reports.
22. Select Notify from the drill-down menu. When selected, this menu will be replaced by a new menu containing a list of users.
23. Select a user.
- When the user gets the notification, a message will be displayed.
24. Change Status - Double-click on the incident on which the status is to be changed, in one of the Incident Management reports.
25. Select Change Status from the drill-down menu. When selected, this menu will be replaced by a new menu containing a list of status codes:
- ASSIGNED - Once an incident has this status, it cannot have additional policy violations added to it. To add policy violations, change the incident status back to Open, add the violations, and then change the status back to Assigned.
  - CLOSED - Once an incident is marked Closed it cannot be modified, and is no longer listed.
  - OPEN - This is the initial status for a new incident.
26. Select the desired status code.
- A message displays when the change has been completed, and the Incident Management panel will be refreshed.
27. Add Comments - Double-click on the incident to which comments are to be added, in one of the Incident Management reports.
28. Select Comments from the drill-down menu, to open the User Comment window. For instructions on how to add comments, see Commenting.

Each user portal displays a My Open Incidents report for that user. From the My Open Incidents report, users can perform the actions shown:

| My Open Incidents                                             |                     |          |          |          |            |           |               |                    |                        |  |
|---------------------------------------------------------------|---------------------|----------|----------|----------|------------|-----------|---------------|--------------------|------------------------|--|
| Start Date: 2007-04-26 09:31:57 End Date: 2007-05-04 09:31:57 |                     |          |          |          |            |           |               |                    |                        |  |
| Incident Number                                               | Timestamp           | Severity | Category | Status   | First Name | Last Name | # of Comments | Count of Incidents |                        |  |
| 4                                                             | 2007-05-03 09:48:24 | INFO     |          | ASSIGNED | dba        | dba       |               |                    | Records: 1 To 1 From 1 |  |

Assign to user...  
 Change Severity...  
 Notify...  
 Change status...  
 Comments...  
 Violations per incident

## Query rewrite

Query rewrite functionality provides fine-grained access control for databases by intercepting database queries and rewriting them based on criteria defined in security policies.

The modification of queries happens transparently and on-the-fly, such that a user issuing queries seamlessly receives results based on rewritten SQL statements.

Query rewrite functionality is implemented through a combination of query rewrite definitions indicating how queries should be changed or augmented and a run-time context indicating the specific circumstances where the query rewrite definitions should be applied.

Rewriting database queries on the fly allows administrators to implement several types of access control, as illustrated by the following examples.

Table 1. Examples of access control with query rewrite.

| Access control                                                                        | Original SQL                     | Rewritten SQL                               |
|---------------------------------------------------------------------------------------|----------------------------------|---------------------------------------------|
| Limiting access to rows by adding a WHERE clause                                      | <code>SELECT C from T</code>     | <code>SELECT C from T WHERE [values]</code> |
| Limiting access to columns by modifying the SELECT list                               | <code>SELECT C1 from T</code>    | <code>SELECT C2 from T</code>               |
|                                                                                       | <code>SELECT C1,C2 from T</code> | <code>SELECT C2 from T</code>               |
| Restricting database activities by rewriting SQL statements to do nothing.            | <code>SELECT EMAIL from T</code> | <code>SELECT++ EMAIL from T</code>          |
| Restricting what users can do by modifying query verbs (SELECT, INSERT, UPDATE, etc.) | <code>DROP TABLE T</code>        | <code>UPDATE T SET [values]</code>          |
| Restricting what users can do by modifying query objects (TABLE, VIEW, COLUMN, etc.)  | <code>SELECT C from T1</code>    | <code>SELECT C from T2</code>               |

The ability to seamlessly rewrite database queries provides an extremely powerful and flexible form of access control that allows organizations to quickly address a wide range of security concerns. For example, query rewrite definitions can be developed to accomplish any of the following:

- Enforcing security in multi-tenancy scenarios where multiple users and applications share a single database, but where not all users and applications should have access to all data.
- Exposing a database to a production environment for testing purposes without exposing the entire database.
- Rapidly correcting critical security vulnerabilities while permanent solutions are developed at the database or application level.

Review the following sections to learn more about how query rewrite works and how to configure it for use within your Guardium® environment.

Note: If the S-TAP is set for `firewall_default_state=1`, the default state for Query Rewrite, `qrw_default_state=1` cannot be set at the same time.

- [How query rewrite works](#)  
Learn how Guardium implements query rewrite functionality.
- [Using query rewrite](#)  
Learn how to enable and use query rewrite functionality.

## How query rewrite works

Learn how Guardium® implements query rewrite functionality.

### Overview

Once query rewrite has been enabled on the S-TAP for supported database servers (see [Enabling query rewrite](#)), query rewrite functionality is implemented through three policy rule actions:

These rule actions are installed as access policy rules. The access policy rules specify both query rewrite definitions that indicate how queries should be rewritten and a run time context that indicates when those definitions should be applied.

Once query rewrite rules have been specified, sessions are handled as follows:

1. An SQL request triggers a QUERY REWRITE: ATTACH rule, and all subsequent activity in the session is watched by query rewrite.
2. While sessions are being watched by query rewrite, traffic is held at the S-TAP and the session information is checked against access policy rules.
3. If a query in the watched session matches a QUERY REWRITE: APPLY DEFINITION rule, the query is rewritten according to the definition and sent to the S-TAP.
4. The S-TAP releases the rewritten query to the database server.
5. When a QUERY REWRITE: DETACH rule is triggered, query rewrite stops watching activity for the remainder of the session or until another QUERY REWRITE: ATTACH rule is triggered.

## Requirements and limitations

Query rewrite is intended to work with the following database servers:

- Oracle
- Db2
- Microsoft SQL

Important: Query rewrite does not support encrypted traffic with Windows S-TAP. Active sessions may be terminated if they are encrypted.

For information about supported database servers and any associated restrictions, see [System requirements](#). For detailed information about database client support for query rewrite, contact IBM Guardium support.

Note: When query rewrite is watching a session, the sniffer is required to send engine verdicts to the S-TAP for each SQL request in the session. This process is asynchronous and introduces latency between the sniffer and S-TAP. Create query rewrite rule conditions that avoid attaching to sessions for performance-sensitive or trusted applications.

## Handling large SQL statements from an MSSQL Server database

Query rewrite does not mask the data when the overwritten SQL is larger than negotiated packet size. In these cases Guardium issues an alert. If the query is too long either a transport-level error occurs or the data in the query is shown as unmasked. If Guardium misses the login packet with the negotiated packet size, then Guardium uses the default packet size as 4K Use the predefined alert QWR Exceptions Alert to be notified of this situation. The alert fires once per session when the query returns more than the negotiated packet size. For more information, see [Predefined alerts](#).

There is a default report QRW Exceptions that provides details of such sessions.

## Related tasks

---

- [Enabling query rewrite](#)
- 

## Using query rewrite

Learn how to enable and use query rewrite functionality.

## About this task

---

Follow this task sequence to enable and begin using query rewrite functionality.

1. [Enabling query rewrite](#)  
Learn how to configure an S-TAP for query rewrite functionality.
  2. [Creating query rewrite definitions](#)  
Learn how to create query rewrite definitions for data masking and access control scenarios.
  3. [Testing query rewrite definitions](#)  
Learn how to test query rewrite definitions against sample input and verify that the rewrite definitions behave as expected.
  4. [Defining a security policy to activate query rewrite](#)  
Learn how to create access policy rules using your query rewrite definitions with live queries.
  5. [Creating a custom report to validate query rewrite results](#)  
Learn how to create a query rewrite tracking report for auditing query rewrite activity.
- 

## Enabling query rewrite

Learn how to configure an S-TAP for query rewrite functionality.

## Before you begin

---

The query rewrite feature is available only when you enable query rewrite in the guard\_tap.ini file and query rewrite policy rules exist and are triggered by session traffic.

## About this task

---

Query rewrite is controlled by a query rewrite parameter in the [TAP] section of the S-TAP guard\_tap.ini file.

## Procedure

---

1. Log on to the database server system using the root account.
2. Stop the S-TAP.
3. Make a backup copy of the guard\_tap.ini configuration file.
  - For Windows - \Program Files\IBM\Windows S-TAP\Bin\
  - For UNIX - /usr/local/guardium/guard\_stap/guard\_tap.ini
4. Open guard\_tap.ini in a text editor.
5. Locate the query rewrite parameter and edit it as required. Set the parameter to 1 to enable it or to 0 to disable it.
  - For Windows - QUERY\_REWRITE\_INSTALLED
  - For UNIX - qrw\_installed
6. Save your changes to guard\_tap.ini.
7. Restart the inspection engines either by navigating to Manage > Activity Monitoring > Inspection Engines and clicking on Restart Inspection Engines; or by logging in to the CLI as user, and restarting the inspection engines using the **restart\_inspection\_engines** CLI command.

## Results

---

When you are done, query rewrite functionality is enabled and responds to policy rules that contain query rewrite actions. For more information about query rewrite parameters, see [Query rewrite parameters](#) for UNIX or [Query rewrite parameters](#) for Windows.

Next topic: [Creating query rewrite definitions](#)

---

## Creating query rewrite definitions

Learn how to create query rewrite definitions for data masking and access control scenarios.

## Procedure

---

1. Go to Protect > Security Policies > Query Rewrite Builder.
2. Provide a unique and meaningful name for the query rewrite definition in the Name field.
3. Create and parse a model query.
  - a. Provide a model query in the Enter a model query field.

For example, to create a rewrite definition preventing the use of **SELECT \* from** statements, enter **SELECT \* from EMPLOYEE** as a model.

- b. Click the DB Type menu and select a SQL parser to use with the model query.
- c. Click Parse to process the model query.

Your model query will be broken down into individual components with each actionable component highlighted with underlined text.

4. Define how to rewrite specific components of the model query.

- a. Click on an underlined component of the parsed query that you would like to rewrite. A dialog opens to help create your query rewrite definition.  
Options:

- Select and modify an individual verb, field, or object from the parsed query
- Add a component to the query (shown as gray underlined text next to the parsed query)
- Rewrite the entire query by clicking the gray underlined [R] next to the parsed query

In the example **SELECT \* from EMPLOYEE** where we want to prevent the use of **SELECT \* from** statements, click the **\*** to provide rewrite content.

- b. The Change from field indicates what will be rewritten.

- c. The To field defines the rewritten component.

For example, to prevent the use of **SELECT \* from** statements, replace the **\*** component with a list of specific objects: **EMPNO, FIRSTNAME, MIDINIT, LASTNAME, WORKDEPT, PHONENO, HIREDATE, JOB, EDLEVEL, SEX**.

Important: Rewrite definitions are based on syntax, so any statement with the form **SELECT \* from [OBJECT]** will match the example. For instance, both **SELECT \* from DEPARTMENT** and **SELECT \* from EMPLOYEE** statements match our example. Query rewrite definitions can be restricted to specific objects using access policy rules. See [Defining a security policy to activate query rewrite](#) for instructions.

- d. Click Save to save the rewrite definition, then click Back to close the dialog.

5. Review the output of the query rewrite definition using the Real time preview field and make any changes as needed.

Using our example, **SELECT \* from EMPLOYEE** is rewritten as **SELECT EMPNO, FIRSTNAME, MIDINIT, LASTNAME, WORKDEPT, PHONENO, HIREDATE, JOB, EDLEVEL, SEX from EMPLOYEE**.

6. When you are satisfied with the results, click Save to save your query rewrite definition.

Your query rewrite definition is saved and displayed in the list of available query rewrite definitions in the Query Rewrite Builder.

## What to do next

---

Continue working with query rewrite definitions:

- Create additional definitions by clicking New and repeating the steps in this task.
- Edit an existing query rewrite definition by double-clicking an item in the list of available query rewrite definitions.
- Copy and edit an existing query rewrite definition by selecting the item in the list of available query rewrite definitions and clicking Clone.
- Delete an existing query rewrite definition by selecting the item in the list of available query rewrite definitions and clicking Delete.

When you are finished working with query rewrite definitions, continue to the next step in this sequence to test and implement your definitions.

[Previous topic: Enabling query rewrite](#)

[Next topic: Testing query rewrite definitions](#)

## Related tasks

---

- [Defining a security policy to activate query rewrite](#)

## Testing query rewrite definitions

---

Learn how to test query rewrite definitions against sample input and verify that the rewrite definitions behave as expected.

### Before you begin

---

To complete this task, you need to have created one or more query rewrite definitions.

### Procedure

---

1. Open Protect > Security Policies > Query Rewrite Builder.
2. Click Set Up Test to open a dialog and select query rewrite definitions for testing.
  - a. Drag and drop items from the Available query rewrite definitions field to the Test query rewrite definitions field.
  - b. Drag and drop items with the Test query rewrite definitions field to order multiple definitions as you would within an access policy.
  - c. Click Save to close the dialog when you are finished.

3. Type or paste test queries into the test field.

For example, to test a rewrite definition preventing the use of **SELECT \* from** statements (see [Creating query rewrite definitions](#)), enter sample queries such as:

```
SELECT * from DEPARTMENT
SELECT * from EMPLOYEE
SELECT FIRSTNAME, case
when SALARY > 150000 then 'high'
when SALARY > 100000 then 'medium'
when SALARY > 80000 then 'fair'
else 'poor'
end from EMPLOYEE
```

```

DELETE from EMPLOYEE where EMPNO=100
INSERT into TEMP_EMP SELECT * from EMPLOYEE

```

4. Click Run Test to process the sample queries and review the results.

For example, the sample queries provided in the previous step return the following results:

Table 1. Query rewrite test results

| Original SQL                                                                                                                                             | Rewritten SQL                                                                                                                                            | Changed |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| SELECT * from DEPARTMENT                                                                                                                                 | SELECT EMPNO, FIRSTNAME, MIDINIT, LASTNAME, WORKDEPT, PHONENO, HIREDATE, JOB, EDLEVEL, SEX from DEPARTMENT                                               | YES     |
| SELECT * from EMPLOYEE                                                                                                                                   | SELECT EMPNO, FIRSTNAME, MIDINIT, LASTNAME, WORKDEPT, PHONENO, HIREDATE, JOB, EDLEVEL, SEX from EMPLOYEE                                                 | YES     |
| SELECT FIRSTNAME, case when SALARY > 150000 then 'high' when SALARY > 100000 then 'medium' when SALARY > 80000 then 'fair' else 'poor' end from EMPLOYEE | SELECT FIRSTNAME, case when SALARY > 150000 then 'high' when SALARY > 100000 then 'medium' when SALARY > 80000 then 'fair' else 'poor' end from EMPLOYEE | NO      |
| DELETE from EMPLOYEE where EMPNO=100                                                                                                                     | DELETE from EMPLOYEE where EMPNO=100                                                                                                                     | NO      |
| INSERT into TEMP_EMP SELECT * from EMPLOYEE                                                                                                              | INSERT into TEMP_EMP SELECT * from EMPLOYEE                                                                                                              | NO      |

Important: Rewrite definitions are based on syntax, so any statement with the form `SELECT * from [OBJECT]` will match the example. For instance, both `SELECT * from DEPARTMENT` and `SELECT * from EMPLOYEE` statements match our example. Query rewrite definitions can be restricted to specific objects using access policy rules. See [Defining a security policy to activate query rewrite](#) for instructions.

5. Continue entering sample queries to test your rewrite definitions.

Click Set Up Test to change or reorder the rewrite definitions used for the test.

## What to do next

When you are satisfied with the test results, create a security policy to begin using your query rewrite definitions with live queries.

Previous topic: [Creating query rewrite definitions](#)

Next topic: [Defining a security policy to activate query rewrite](#)

## Related tasks

- [Defining a security policy to activate query rewrite](#)
- [Creating query rewrite definitions](#)

## Defining a security policy to activate query rewrite

Learn how to create access policy rules using your query rewrite definitions with live queries.

## Before you begin

To complete this task, you need to have created and tested one or more query rewrite definitions, and you need to be familiar with creating security policies.

## Procedure

1. Open Protect>Security Policies>Policy Builder.
2. Create a new policy or modify an existing policy to use your query rewrite definitions.  
Tip: Consider creating a new policy for testing query rewrite definitions. Add your rewrite rules to existing security policies once you are satisfied with the behavior of the test policy.
3. Click Edit Rules to begin adding rewrite rules to the selected policy, then select Add Rules>Add Access Rule.  
Note: Query rewrite rules are always classified as access rules.
4. Add a rule with a QUERY REWRITE: ATTACH rule action. Be sure to check the Continue to next rule checkbox. This rule identifies the specific session parameters that must be matched in order to trigger a query rewrite session, for example a specific database user name or client IP address.
5. Add a rule with one or more QUERY REWRITE: APPLY DEFINITION rule actions and select the query rewrite definition(s) you would like to apply. This rule identifies the specific objects or commands that must be matched in order to apply the rewrite definitions and modify the source query.  
For example, you can limit the data that displays back to a user when a `SELECT * from EMPLOYEE` query is issued. To do so, set the Object field to `EMPLOYEE` and create a query rewrite definition to replace the `*` with a list of defined columns for the data you want the user to have access to.
6. Add a rule with a QUERY REWRITE: DETACH rule action. This detaches the query rewrite session and prevents further monitoring of session traffic. The conditions set for the detach rule should not be the same as the attach rule.
7. To install the new policy, return to the Policy Finder, select your security policy, and choose Select an installation action>Install and Override. Click OK when asked to confirm installation of the policy.
8. Log in to your database server and run test queries to verify that your access policy rewrite rules are functioning as intended.
  - a. Log in to your database server.
  - b. Issue queries that should trigger (or should not trigger) the installed access policy rules and match the criteria of your query rewrite definitions.  
For example, if you set the Object to `EMPLOYEE` and you issue `SELECT * from EMPLOYEE`, you should only see results for the columns you defined for `*` in the query rewrite definition. In contrast, if you issue a `SELECT * from DEPARTMENT`, you should see all column data returned for the `DEPARTMENT` object.
  - c. Verify that the results reflect the rewritten SQL.

Previous topic: [Testing query rewrite definitions](#)

## Related concepts

---

- [Policies](#)

## Creating a custom report to validate query rewrite results

---

Learn how to create a query rewrite tracking report for auditing query rewrite activity.

### Before you begin

---

To complete this task, you need to have created and installed access policy rules that apply query rewrite definitions, and you need to be familiar with creating reports.

### About this task

---

A query rewrite tracking report helps validate query rewrite actions in both test and production environments.

### Procedure

---

1. Follow instructions in [Using the Query-Report Builder](#) to create a new query.
2. Select one of the main entities:
  - Query Rewrite Log
  - Client/Server
  - Session
  - Access Period
3. Include the following items as a starting point for your query rewrite report:
  - Client/Server: Timestamp
  - Client/Server: DB User Name
  - Client/Server: Server Type
  - Query Rewrite Log: Applied QR Definition Names
  - Query Rewrite Log: Input SQL
  - Query Rewrite Log: Output SQL
4. Save the report when complete.
5. Click Add to My Custom Reports to add the report to your custom reports.
6. Open Reports > My Custom Reports and select the report you created to view a report of query rewrite actions.

Previous topic: [Defining a security policy to activate query rewrite](#)

---

## File Activity policies for UNIX and Windows file servers

---

File activity policies are used to protect sensitive data on UNIX file servers, Windows file servers,

- [Using rules for file activity policies](#)

A file activity monitoring policy specifies how Guardium handles different file activity events. Each policy consists of a set of ordered rules. Each rule in a policy defines a conditional action that is taken when the rule matches. The conditional test can be simple, for example a user accesses a specific location, or a complex test that considers multiple conditions. The action ranges from nothing to blocking the event. Multiple grouping and alerting actions can be combined and ordered to create sophisticated responses to matched rules.

- [Create a FAM policy and its rules from scratch for Windows and UNIX servers](#)

Set up file activity monitoring by defining and managing policies and rules in the Policy Builder for Files window.

- [Creating a FAM policy rule from the Investigative Dashboard Entitlements tab](#)

You can use the monitored data, such as datasource names, user names, actions, and file paths, in the Investigation Dashboard Results Table to create policy rules.

## Using rules for file activity policies

---

A file activity monitoring policy specifies how Guardium handles different file activity events. Each policy consists of a set of ordered rules. Each rule in a policy defines a conditional action that is taken when the rule matches. The conditional test can be simple, for example a user accesses a specific location, or a complex test that considers multiple conditions. The action ranges from nothing to blocking the event. Multiple grouping and alerting actions can be combined and ordered to create sophisticated responses to matched rules.

You can, for example, define policies for these cases:

- Log a policy violation if John writes into the CONFIDENTIAL folder
- Block a group of users from deleting the file SALARIES.XLS
- Send an e-mail to Krishna if JENNY reads from any files that begin with the name sample\*
- Audit all accesses to any file that has been classified as containing sensitive data related to PCI

### Groups

Guardium uses the concept of groups for policy and report creation.

Guardium groups are created and maintained on the Guardium collector or Central Manager. Do not confuse Guardium groups with file system groups.

It is recommended that you consider a naming strategy for your groups, including groups of data sources (file servers), groups of files (such as by sensitivity level or combination of sensitivity level and application), groups of users (a list of all known users, "authorized" users, users with special privileges).

Guardium groups are created and maintained on the Guardium collector or Central Manager. Do not confuse Guardium groups with file system groups.

#### Rule Guidelines

- A overly broad rule (a rule that monitors too many files) can overload the system and increase processing and response time.
- A FAM rule can have more than one pattern in it. To protect both a directory and its contents, define a rule with two patterns /FAMtest/\* and /FAMtest.
- A group comprised of file paths: each path must be unique irrespective of case. For example, these two paths can co-exist in a group: C:\ABC and C:\abcdef. However, these two paths cannot co-exist in a group C:\ABC and C:\abc. The Group builder is not case sensitive. It is not required to input members with all upper case characters or all lower case characters. However, in UNIX, which is case sensitive, the path /IBM/Guardium is different from the path /ibm/guardium. If the user wants to monitor both of these paths, the current Group builder has a limitation and will not see them as two paths.
- The ordering of rules in the security policy is very important. The rules are sent to the S-TAP as a set and are processed strictly in order. Any given user activity is checked against each rule in the policy in order. The first rule that meets the criteria of this file access is applied and subsequent rules are ignored. In most cases, put the most specific rule first and the most general rule last. For example, you have two rules:
  - **Rule A:** audit only all access to /data/\*
  - **Rule B:** block, log violation and audit user 'joe' from accessing /data/salaries

If you put Rule A first, and Joe tries to read /data/salaries, there is no need to go to the next rule, and Joe will be audited. If you put Rule B first, Joe is blocked from accessing /data/salaries and there is no need to go to the next rule.

#### Rule attributes

##### Rule name

A unique name.

##### Datasource

The datasource can be:

- Datasource selected from drop-down list
- Group selected from drop-down list
- Group created from selected groups in the Create New Rule window
- Manually entered path

##### Rule Action

The rule action is the action taken when the criteria are met. Actions are defined for:

- One action for any file access that matches the rule criteria
- Multi-action rule comprised of multiple actions, each one is per a specified command category or a specified group. Note that **Continue to next rule** is not supported when using Multi-action rules.

The rule actions are:

- Alert and audit: Send an alert directly generated from the sniffer with specific behavior, and log the event.
- Audit only: Log the event in GDM tables
- Block, log violation, and audit: Block access to the object, log a policy violation, and log the event. A blocking action requires an alert configuration as well.
- Ignore: No action taken.
- Log as violation and audit: Log this as a policy violation and log the event.

#### Notification types

- Email messages: You can specify a Guardium user email, or an external email. Emails are sent using the SMTP server configured for the Guardium system.
- SNMP traps: alerts the trap community configured for the Guardium system.
- Syslog messages: generates messages that are written to the syslog.
- Custom notifications: user-created notification handlers implemented as Java classes.

##### Rule criteria

For any given file access, rule criteria are used to evaluate whether a particular action should be taken. For any datasource or group of datasources (file servers), the rule criteria that you can specify include:

**User:** The OS user who is accessing files. This can also be a group of users, as defined in a Guardium group. If this is left blank then the rule applies to all users (except root).

**File Path:** This can be a Windows or UNIX file path, an individual file path, or a group of file paths, as defined in a Guardium group. This cannot be blank (except when removable media is selected). You can also select to monitor the subdirectories in the file path.

Wild cards in the name specification:

- The '\*' character matches any number of any characters
- The '?' character matches one single character
- For UNIX, use back slash to escape \* and ?

Tip: Wild cards take extra processing. Excessive use of wild cards impacts performance.

This matches. The file name, FAM.output, matches the name, FAM, and is located in a subdirectory of the given directory '/'.

#### UNIX

Usage:

- To match all files on disk, enter /\*
- To match /tmp/My\*File.txt exactly , use /tmp/My\\*File.txt
- To match any file with a .txt extension in /tmp, use /tmp/\*.txt

Example: The FAM rule pattern is: /FAM\*

meaning

- Directory: /
- File name: FAM\*

The rule in place has subdirectories selected: (Subdirs: Yes)

The file accessed is: /guardium/modules/SUPERVISOR/10.0.0/FAM.output

**Windows:** For Windows, you must specify the drive, such as C:\

Usage:

- To monitor all files on the C drive, enter C:\ and mark the Monitor subdirectories checkbox.
- To match any file with a .txt extension in C:\tmp, use C:\tmp\\*.txt

GuardAPI examples: create policy with two rules

```
grdapi create_policy ruleSetDesc=policy1 isFam=true
grdapi create_fam_rule policyName=policy1 ruleName=rule1 serverHost="x.x.x.x" filePath="/famtest/*" command="DELETE"
actionName="Alert and Audit" notificationType="SYSLOG"
grdapi create_fam_rule policyName=policy1 ruleName=rule2 serverHost="x.x.x.x" filePath="/famtest/*" command="READ"
actionName="Alert and Audit" notificationType="MAIL"

policy1 -> rule1 -> "DELETE" -> "Alert and Audit" -> "SYSLOG"
policy1 -> rule2 -> "READ" -> "Alert and Audit" -> "MAIL"
```

GuardAPI examples: create policy with multi-Action Rule

Multi-Action Rule for FAM - Multi-action rules are comprised of multiple actions, each one is per a specified command category or a specified group. The commands in a FAM context are: Read, Write, Delete, Execute and File Operation. If the system does not support Multi-Action Rules, it ignores the rule and continues to the next rule.

```
grdapi create_policy ruleSetDesc=policy1 isFam=true
grdapi create_fam_rule policyName=policy1 ruleName=rule1 serverHost="x.x.x.x" filePath="/famtest/*"
add_action_to_fam_rule policyName=policy1 ruleName=rule1 command="DELETE, READ" actionName="Alert and Audit"
notificationType="SYSLOG"
add_action_to_fam_rule policyName=policy1 ruleName=rule1 command="WRITE" actionName="Alert and Audit"
notificationType="MAIL"

policy1 -> rule1 -> "DELETE, READ" -> "Alert and Audit" -> "SYSLOG"
policy1 -> rule1 -> "WRITE" -> "Alert and Audit" -> "MAIL"
Adding another action using commandGroupId, assuming commandGroupId=20000 exists, and it has "DELETE, WRITE"

add_action_to_fam_rule policyName=policy1 ruleName=rule1 command="READ" commandGroupId=20000 actionName="Ignore"
notificationType=""

policy1 -> rule1 -> "READ, DELETE, WRITE" -> "Ignore"
```

## Create a FAM policy and its rules from scratch for Windows and UNIX servers

Set up file activity monitoring by defining and managing policies and rules in the Policy Builder for Files window.

### About this task

Once you open the Policy Builder for Files and additional views within the policy builder, you can toggle between the various views by clicking Policy Builder for Files, New Policy and Create New Rule at the bottom of the page.

You can also create policies and rules using the API.

### Procedure

1. On a standalone or MU, access the FAM policy builder. Go to Protect > Security Policies > Policy Builder for Files.
2. Click to open the New Policy page.
3. In the Type field, select Windows, Linux, and Unix systems.
4. In the Policy Name field, type a name for the policy. (You can save the policy once a rule is defined.)
5. To add existing rules to the policy.
  - a. Click Show Templates. The Rule Templates table opens.
  - b. Optionally filter the list with the filter function.
  - c. Select one or more rules and click the right arrow
6. To create a new rule.
  - a. Click to open the Create New Rule page.
  - b. In the Rule name section, type the name.
  - c. In the Choose datasources section, specify a datasource manually, by selecting from a list of datasources, or by selecting a group of datasources. See [Datasource](#) and [Groups](#).
  - d. In the Define rule criteria to include or exclude file paths, optionally to monitor the subdirectories in the file path or to monitor removable media. See [Rule criteria](#).
  - e. In the Define rule action section, define the rule action. See [Rule Action](#).
7. Click Save.
8. To modify an existing rule and add it to the policy.
  - a. In the New Policy page, click Show Templates.
  - b. Under Rule Templates, select the rule and click .
  - c. Under Rule, select the rule and click , change the name, modify the other attributes as relevant, and click Save.
9. Change the order of the rules using the and .
10. Delete a rule by selecting it and clicking .
11. Click Save to save the policy, or Save and Install to install the policy immediately. (See [Using the Policy Installation tool](#)).

## Related reference

---

- [File Activity Monitor APIs](#)

## Creating a FAM policy rule from the Investigative Dashboard Entitlements tab

You can use the monitored data, such as datasource names, user names, actions, and file paths, in the Investigation Dashboard Results Table to create policy rules.

### Before you begin

---

- The FAM bundle must be installed and configured
- Discovery and classification must be enabled
- Investigation Dashboard must be enabled, see [Enabling and disabling the Investigation Dashboard](#)

### Procedure

---

1. Choose File from the dropdown list in the product banner and click the search icon to open the Investigation Dashboard for file data.
2. Open the Results Table Entitlements tab. Click Details to see individual entries.
3. Choose one or more entries in the results that you want to use to populate a rule. You can use the Select all check box to include all the entries that are currently displayed (not all the entries in the database).
4. Right-click and choose Add Policy Rule.  
The Build Rule dialog opens with values from the entries that you selected. If you selected multiple entries, a group is created that contains the values from those entries. You can create a rule that is to be added to an existing policy, or create a new policy that includes your new rule.  
Note: A overly broad rule (a rule that monitors too many files) can overload the system and increase processing and response time.  
Note: A FAM rule can have more than one pattern in it. To protect both a directory and its contents, define a rule with two patterns /FAMtest/\* and /FAMtest.  
Note: When using FAM policy, setting a group to define monitored file paths requires either consideration of case sensitivity. Otherwise the group cannot be created successfully. The workaround is to create two different FAM policy rules. Clarification - If strings defined as members of group are different without considering case sensitive, the group can be created successfully. For example: 1. C:\ABC 2. C:\abcdef. If strings defined as members of group are same without considering case sensitive, the group can NOT be created. For example: 1. C:\ABC 2. C:\abc So it is not required to input members with all upper case characters or all lower case characters. Group builder is not case sensitive. However, in UNIX, which is case sensitive, the path /IBM/Guardium is different from the path /ibm/guardium. If the user wants to monitor both of these paths, the current Group builder has a limitation and will not see it as the same path.
5. Choose datasources, actions, and criteria. Overwrite any values that you want to change. Click Edit to modify each field.
6. To create a new policy and install it, click Create and Install. To create the policy but not install it, click OK.

## File activity policies for network-attached storage (NAS) and SharePoint

---

Set up file activity monitoring for NAS devices and SharePoint by defining policies and rules in the Policy Builder for Files.

- [Creating file activity policies for network-attached storage \(NAS\) devices](#)  
Use the Policy Builder for Files to set up file activity monitoring for NAS devices. You can configure multiple monitored hosts on the same server. Each monitored host can have its own policy configuration by using a distinct datasource.
- [Creating file activity policies for SharePoint](#)  
Use the Policy Builder for Files to set up file activity monitoring for SharePoint.
- [Creating a DAM access policy to monitor files on NAS and SharePoint](#)  
Use the comprehensive criteria and rule actions of Data Activity monitoring (DAM) access policy to monitor FAM for NAS and SP in deeper granularity. Set up alerts on a subset of users, audit all or a set of users, and optionally ignore a set of users or operations.

## Creating file activity policies for network-attached storage (NAS) devices

---

Use the Policy Builder for Files to set up file activity monitoring for NAS devices. You can configure multiple monitored hosts on the same server. Each monitored host can have its own policy configuration by using a distinct datasource.

### About this task

---

After you establish a connection between your monitoring agent and the Guardium system, you can configure FAM for NAS by using the Policy Builder for Files.  
Note: You can no longer configure FAM for NAS using the configuration app. Any manual change to the configuration file triggers an alert.

### Procedure

---

1. Go to Protect > Security Policies > Policy Builder for Files.
2. Click to create a new policy.
3. To enter the type of policy, click the drop-down box and select Network Attached Storage.
4. Enter a name for the new policy. The policy can be saved after a rule is defined.
5. To add existing rules to the policy:
  - a. Click Show Templates. The Rule Templates table opens.
  - b. Optionally filter the list with the filter function.
  - c. Select one or more rules and click

6. To create a new rule:
    - a. Click  to open the Create New Rule window.
    - b. Name the rule, and click Next.
    - c. Specify a datasource manually, by selecting from a list of datasources, or by selecting a group of datasources and click Next.
  7. Define rule criteria by including or excluding file paths, excluding accounts, or file extensions.
  8. Select the Specify action for specific operation or group checkbox to specify the operations that require monitoring, and the appropriate rule action. If the check box is not selected, all operations are monitored by default.  
Note: The operations that are selected override the settings on the configuration app of the monitoring agent.
  9. To configure an existing rule:
    - a. Click  to change the name, modify the other attributes as relevant, and click Save.
    - b. Delete a rule by selecting it and clicking .
10. Click Save to save the policy, or Save and Install to install the policy immediately. For more information, see [Using the Policy Installation tool](#).
- Attention:  
In Guardium® v11.2 and later, NAS datasources appear in the following format: <The name of the server where the agent is installed>:<the monitored host>\_<type of NAS device>:FAM-NAS.
- When FAM for NAS is upgraded to v11.2 or later, the existing policies that are installed on v11.0 or v11.1 do not work due to the change in the datasource format. To resolve this issue, update the name of the NAS datasource, save, and reinstall the policy.

## Creating file activity policies for SharePoint

Use the Policy Builder for Files to set up file activity monitoring for SharePoint.

### About this task

After you establish a connection between your monitoring agent and the Guardium system, you can configure FAM for SharePoint by creating and installing a policy.  
Note: You can no longer configure FAM for SharePoint using the configuration app. Any manual change to the configuration file triggers an alert.

### Procedure

1. Go to Protect->Security Policies->Policy Builder for Files.
  2. Click  to create a new policy.
  3. To enter the type of policy, click the drop down box and select SharePoint.
  4. Enter a name for the new policy. The policy can be saved after a rule is defined.
  5. To add existing rules to the policy:
    - a. Click Show Templates. The Rule Templates table opens.
    - b. Optionally filter the list with the filter function.
    - c. Select one or more rules and click .
  6. To create a new rule:
    - a. Click  to open the Create New Rule window.
    - b. Name the rule, and click Next.
    - c. Specify a datasource manually, by selecting from a list of datasources, or by selecting a group of datasources and click Next.  
SharePoint datasources appear in the following format: <The name of the server where the agent is installed>:FAM-SP.
  7. Define rule criteria by entering the site URL. Exclude accounts, if appropriate..
  8. Select the Specify action for specific operation or group check box to specify the operations that require monitoring, and the appropriate rule action. If the check box is not selected, all operations are monitored by default.  
Note: The operations that are selected override the settings on the configuration app of the monitoring agent.
  9. To configure an existing rule:
    - a. Click  to change the name, modify the other attributes as relevant, and click Save.
    - b. Delete a rule by selecting it and clicking .
10. Click Save to save the policy, or Save and Install to install the policy immediately. For more information, see [Using the Policy Installation tool](#).

## Creating a DAM access policy to monitor files on NAS and SharePoint

Use the comprehensive criteria and rule actions of Data Activity monitoring (DAM) access policy to monitor FAM for NAS and SP in deeper granularity. Set up alerts on a subset of users, audit all or a set of users, and optionally ignore a set of users or operations.

### Before you begin

Create and install a FAM policy to filter FAM traffic that you want to monitor. For more information, see [Creating file activity policies for network-attached storage \(NAS\) devices](#) and [Creating file activity policies for SharePoint](#).

Note: Set the FAM policy action to Audit Only.

### About this task

Apply Data Activity Monitoring (DAM) access policy to NAS and SharePoint to achieve granular policy filtering.

## Procedure

---

1. Go to Protect > Security Policies > Policy Builder for Data.
2. Create a policy by clicking the  icon.
3. From the Name and properties pane of the Create New Policy window, set the policy type to Data security policy and define a policy name.
4. Click the Rules pane to begin working with policy rules. Create a rule by clicking the  icon.
  - a. From the Rule definition pane of the Create New Rule window, define a Rule name. Set the Rule type to Access.
  - b. Click the Rule criteria pane. Use the menus to select individual parameters, define selection operators, and then specify values or groups to match.  
For FAM for NAS and SharePoint, use the following criteria:
    - Session level criteria
      - Operating system user: The username of NAS or SharePoint. The database username is also the same.
      - Client IP address: The IP address that is used to connect to NAS or SharePoint.
      - Server IP address: The IP address where the NAS or SharePoint server is hosted.
      - Server host name: The hostname of the NAS or SharePoint host
      - Service name: To process FAM for NAS traffic, use NASFAM. For SharePoint, use SPFAM.
    - SQL criteria
      - i. Command  
Note: Commands are case-sensitive.  
For NAS, use the following commands:
        - Rename
        - Update
        - Create
        - Read
        - Delete
        - Access Rights ChangeFor SharePoint, use the following commands:
        - CheckOut
        - CheckIn
        - View
        - Delete
        - Update
        - ProfileChange
        - ChildDelete
      - ii. Object
        - For NAS, provide the absolute path of the file name or directory name.
        - For SharePoint, provide the full URL to the SharePoint object.

Attention:

When both DAM and FAM for NAS and SP policies are installed to monitor NAS and SharePoint traffic, FAM rules are evaluated and triggered last, regardless of the order of the policies.

Enable Continue to next rule for all DAM policy rules to ensure that the FAM rules are triggered.

- c. Click the Rule action pane to begin working with rule actions, then create a new rule action by clicking the  icon.  
For FAM for NAS and SharePoint, use the following actions:
  - ALERT PER MATCH
  - ALERT DAILY
  - ALERT ONLY
  - ALERT PER TIME GRANULARITY
  - LOG MASKED DETAILS
  - LOG FULL DETAILS
  - LOG FULL DETAILS WITH REPLACED VALUES
  - SKIP LOGGING
  - LOG ONLY
- Note: FAM for NAS and SharePoint does not support actions that are tracked per session or require S-TAP.
- d. After the rule is defined, click OK to return to the Rules pane.  
Continue working with rules as needed.

5. After the policy and its rules are defined, click OK to save the policy and return to the Security Policies table.

---

## Configuring consolidation of FAM MS Office events

Use the FAM monitor Office event consolidation feature to filter out the extraneous, irrelevant MS Word, Excel, and PowerPoint file activities.

When FAM monitors MS Office products MS Word, Excel, and PowerPoint, it generates a lot of extraneous and confusing file events that make it difficult to determine what actually happened in the system. You can use the Office event consolidation feature to filter out the extraneous, irrelevant file activities so that only a clear concise stream of useful events is presented to the collector. The filter eliminates a very high percentage of extraneous events out of the data stream, although occasionally an extraneous file event could be reported. For instance, Windows and Office open files multiple times to read file attributes without ever actually loading the file into memory. For Office this occurs when a user opens a file. Office initially opens and closes the file to read its attributes (which generates a READ event) before actually reading the file into memory (which generates another READ event). Unfortunately it is impossible to distinguish opening a file to read its attributes, from Office opening and reading the actual file into memory.

The FAM monitor office filter software filters out all activity done to temporary files, all activity done to the office journaling files, and the majority of other events that don't represent what the end user actually did. It also eliminates a lot of the ambiguity as to what happened on the system by providing a much finer granularity of file events. For instance, instead of FILEOP events, it reports the actual underlying events that make up the FILEOP, namely RENAME FILE, SET FILE PERMISSIONS, and SET FILE PROPERTIES. There are also separate events for activity that occurs to folders. This includes CREATE FOLDER, OPEN FOLDER, CLOSE FOLDER, RENAME FOLDER, READ

FOLDER, WRITE FOLDER, EXECUTE FOLDER, DELETE FOLDER, SET FOLDER PERMISSIONS, and SET FOLDER PROPERTIES. These are the same events that are generated for files – the only difference is that they apply to folders instead.

The OPEN FILE, CLOSE FILE, OPEN FOLDER, and CLOSE FOLDER events are processed locally by the FAM monitor but are **not** delivered to the collector. The reason that they are not delivered to the collector is that the Windows file explorer program is constantly opening and closing files in the background and these events are rarely useful or desirable to have. Reporting all of them to the collector would essentially provide useless information to the end user and would flood the collector and the network with useless traffic.

The Office event consolidation is configured with these parameters, in the guard\_tap.ini file. The parameters apply only to FAM monitoring; they are ignored by the S-TAP.

To modify the guard\_tap.ini file:

1. Log on to the database server system using the root account.
2. Stop the S-TAP.
3. Make a backup copy of the configuration file: guard\_tap.ini. The default file locations is \Program Files\IBM\Windows S-TAP\Bin\
4. Open the configuration file in a text editor.
5. Edit the file as necessary. These parameters must be in the [Tap] section of the file.
6. Save the file.
7. Restart the S-TAP.

| Parameter Name        | Possible Values                                                               | Default Value                                      | Description                                                                                                                                                                                                                                                                                                                          |
|-----------------------|-------------------------------------------------------------------------------|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ENABLE_OFFICE_FILTERS | 0, 1                                                                          | 1                                                  | Enables or disables the office filter component of the FAM monitor software. When disabled, all files events are reported to the collector including those for temporary files, journaling files, etc. When enabled, only useful files events related to the actual operation the end user performed are delivered to the collector. |
| WORD_EXTENSIONS       | List of file extensions<br>.docx .doc<br>.docm .dotm<br>.dotx .dot .odt       | .docx .doc<br>.docm .dotm<br>.dotx .dot .odt       | The file extensions that identify a file as a Microsoft Office Word source file. The FAM monitor software uses the office filter component on the event streams generated for these files.                                                                                                                                           |
| EXCEL_EXTENSIONS      | List of file extensions<br>.xlsx .xls .xlsm<br>.xlsl .xltx .xltm<br>.xlt .ods | .xlsx .xls .xlsm<br>.xlsl .xltx .xltm<br>.xlt .ods | The file extensions that identify a file as a Microsoft Office Excel source file. The FAM monitor software uses the office filter component on the event streams generated for these files.                                                                                                                                          |
| POWERPOINT_EXTENSIONS | List of file extensions<br>.pptx .pptm .ppt<br>.potx .potm .pot<br>.odp       | .pptx .pptm .ppt<br>.potx .potm .pot<br>.odp       | The file extensions that identify a file as a Microsoft Office PowerPoint source file. The FAM monitor software uses the office filter component on the event streams generated for these files.                                                                                                                                     |
| FSM_LOG_EVENTS        | 0, 1                                                                          | 0                                                  | Enables or disables the logging of file events to the FAM monitor text log file. When enabled, all events like CREATE FILE, READ FILE, etc. that are sent to the appliance are also logged to the application's circular text log file in the STAP ..\logs folder.                                                                   |

## Investigation Dashboard for data

The investigation dashboard is a preset group of charts and a table that help you understand what is happening in your system at any given time, and upon which you can build your own customized dashboards.

There are four default views for data activity monitoring, each with different charts and tables. Select the view from the dashboard menu . The default views cannot be modified.

The default dashboards contain data for the last hour presented in one or more of:

- Trimetric charts (3-axis data graphs). The default view is a color map. Additional views are bar graph, bubble graph, line graph, pie graph, step graph, and area graph.
- Results table: provides the search results and investigation features of the original quick search. The Results Table is always at the bottom of the dashboard. It can be added to any dashboard. Tabs are:
  - Activity: Summary and Details tabs. Each row in the Summary tab gives the number of instances of recorded activities per server-DB pair and the number of DB types. The Detailed Summary adds the count of Source Programs, DB users, OS users, Client hostname, Client IP, and date. Each row in the Details tab gives full details on one activity.
  - Outliers Summary and Details tabs: see [Interpreting data outliers in the investigation dashboard](#).
  - Errors Summary and Details tabs: Summary and Details tabs. Each row in the Summary tab gives the number of instances of reported errors per server and the number of DB types and DB users. The Detailed Summary adds the number of Client IPs, error types and dates. Each row in the Details tab gives full details on one error.
  - Violations Summary and Details tabs. Each row in the Summary tab gives the number of instances of recorded violations per server-DB pair and the number of DB types. The Detailed Summary adds the count of Source Programs, DB users, OS users, Client hostname, Client IP, severity, violation, and date. Each row in the Details tab gives full details on one violation.
  - Vulnerability Assessments Summary and Details tabs. These tabs show the last results per VA test. For example, a test that runs daily has daily updated results. The data is kept for 90 days. If a test wasn't executed during the last 90 days, the results are purged.

You can export the data in individual tabs to CSV and PDF. A comma in the data results corrupts the export to CSV, and data results can shift by one column.

Additional views that you can add or open, all from the Add Chart drop-down except the topology view:

- Topology view  : see [Using the topology view](#)
- Animated bubble chart: an animated visualization of data changes over the last 48 hours. The chart depicts the behavior of objects over a period of 24 hours. Each object is depicted as a circle, and its area and position (x and y axis) represent three user-selected variables. The animation represents the object's behavior over the 24 hours. Access from the Add Chart drop-down.
- Sankey chart: This chart presents four dimensions (and their relationships) in one view, giving a more complete and fluid view on the data. It is an extremely useful graph for investigating filtered data of a specific Alert, Outlier, Report, and Threat. See [Using the Sankey chart](#)
- Activity chart: a line chart that displays the volume of activity and outliers, located above the Results table. Access from the Add Chart drop-down.
- Data in-sight: 3D visualization of data activity, see [Using Data In-Sight](#).

Controls and options on this page:

- A categorized facet list of Where, Who, What, Exception, and When, from the search results, appears on the left side of every dashboard and cannot be removed. Filter the entire dashboard by the specific facets, by expanding the list and clicking individual facets.
- The Active Filters row at the top of the window shows the current filters. Delete filters by clicking the .
- Big Data Intelligence only: Select Guardium System or GBDI - Guardium Big Data Intelligence.
- Search field: free text search that filters the results in all fields simultaneously, irrespective of facet and no case-sensitivity. Exceptions:
  - Anomaly score does not support < or >
  - Searching in a specific field is case-sensitive. For example, when searching "Source Program=nnnnn" nnnn must match a value in the facets.
  - Escaping backslash (\) characters: To correctly escape a backslash character for use in a query condition, use two backslash characters. For example, to specify domain\user you need to enter domain\\user.
  - The summary tabs do not support free search.
-  Distributed search: see [Local and distributed search](#)
- Time period for which data is presented: modify by clicking the drop-down in the upper right corner. Options are last 1 hour, last 3 hours, last 1 day, last 3 days, any time period you specify. Default is one hour. If you select GBDI - Guardium Big Data Intelligence, the time period options are last 1 day, last 3 days, last 1 week, last 3 weeks, any time period you specify. The time period includes a time zone setting, by default the current Guardium system's time zone. Data is reported according to this time zone.
- Filters drop-down: see [Filtering data and saving filters in the investigation dashboard](#)
-  : see [Creating, saving, and exporting investigation dashboards](#)

## Related concepts

- [Interpreting data outliers in the investigation dashboard](#)
- [Big Data Intelligence](#)
- [Assessments](#)

## Related tasks

- [Using the topology view](#)
- [Using Data In-Sight](#)

## Filtering data and saving filters in the investigation dashboard

### About this task

You can filter data in the entire investigation dashboard, and in an individual chart. You can drill down from the Results Table into related information.

You can save filters for your future use. When you save a filter set, you choose if you want to share it, and choose the roles that you share it with.

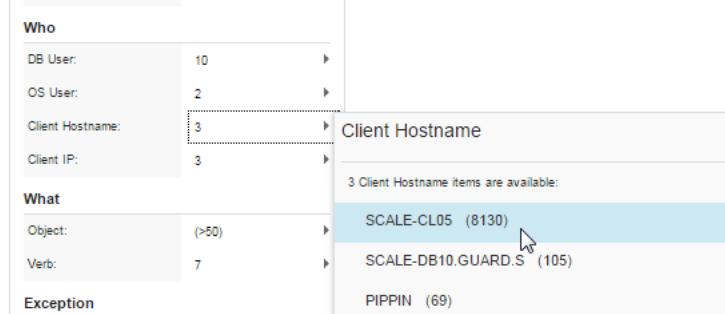
### Procedure

1. Use the rules and syntax to filter data. All of these are relevant for both the Details and Summary tab, except where noted.
  - To match an exact phrase, use double quotation marks around the search terms. For example, "**Profiling Alert List**" returns entries for Connection Profiling Alert List but not for Profiling List Alert.
  - To match all specified search terms, separate the terms with a space. For example, **Hadoop getlisting** returns any entries that contain both Hadoop and getlisting in any location or sequence.
  - To match any specified search terms, separate the terms with OR or a vertical bar (|). For example, **Hadoop OR getlisting** returns any entries that contain either Hadoop or getlisting in any location.
  - To exclude a specified search term, use NOT or a period (.). For example, **NOT Hadoop** does not return any entries that contain Hadoop in any location.
  - Wildcards are supported by using asterisks (\*) at the beginning or ending of a string. For example, **10.10.70.\*** returns any entries with the string 10.10.70. followed by any additional characters.
  - Search rules can be used in combination. For example, **2016-5-08 (19.\*|20.\*)** returns results in the time range of May 8 between the hours of 19:00:00 – 20:59:59.
  - To match an exact phrase in a specific column, enter "**field name=value**", for example "**DB USER=user123**". This search syntax is the only case-sensitive syntax. In the Details tab, you can also use this search for columns with numeric values with search values of < >. For example, "**Total Instances>1**". This is particularly useful when there results on multiple pages and you cannot see the full list of possible values.

Adding filters changes each view based on the *RefFilter* specified for the view. Current filters appear in the menu bar. Each one can be cleared by clicking its X.

2. Refine search results with any of the following methods:

- Select specific filters based on the facets list:



- Click the x or y-axis headers of a chart.
- Click an individual search result in the Results Table:

| Source Program     | DB User  | OS User | Client Hostname |
|--------------------|----------|---------|-----------------|
| DB2JCC_APPLICATION | DB2INST1 |         | PIPPIN          |
| DB2JCC_APPLICATION | DB2INST1 |         | PIPPIN          |
| DB2JCC_APPLICATION | DB2INST1 |         | PIPPIN          |

Note: You can select one or more rows and right-click one of the server/DB user/Client IP cells to add them to an existing group, or to create a new group.

3. Drill down by individual results by right-clicking on specific search results and exploring related outliers, errors, or violations, or viewing one of several available drill-down reports.

| Source Program     | DB User  | OS User | Client H |
|--------------------|----------|---------|----------|
| DB2JCC_APPLICATION | DB2INST1 | PIPPIN  |          |
| DB2JCC_APPLICATION | DB2INST1 |         |          |
| DB2JCC_APPLICATION | DB2INST1 |         |          |
| DB2JCC_APPLICATION | DB2INST1 |         |          |

4. To save a filter set, click **Filters > Save**. Provide a name for the filter and mark it as Private or click Share with to share the filter with specific roles. To save as your default filter set (dashboard always opens with these filters), select Set as default filter. When you are finished, click OK to save the filter.

## Monitor and audit

After you identify your sensitive data and take steps to protect it, you must monitor activities that access this data. In many cases you can use the data that is generated by monitoring to comply with audit requirements, either regulatory or internal.

- **[Enabling and disabling the Investigation Dashboard](#)**

This topic describes how to enable and disable the Investigation Dashboard.

- **[Basic data security monitoring policy](#)**

Use the basic data security monitoring policy to get started with Guardium SQL traffic monitoring.

- **[Smart assistant for compliance monitoring](#)**

The compliance monitoring smart assistant helps you quickly configure monitoring for GDPR, PCI, SOX, and other security standards and regulations.

- **[Investigation Dashboard](#)**

The Investigation Dashboard provides powerful tools for identifying and assessing problems that might exist in your Guardium® environment. It uses either local or system-wide unfiltered data, and provides numerous filter options to query data across an entire Guardium environment, potentially from any Guardium collector within that environment.

- **[Threat Detection Analytics](#)**

Guardium includes specialized threat detection analytics that scan and analyze audited data to detect symptoms that may indicate different types of database attacks.

- **[Data Protection Dashboard](#)**

The Guardium data protection dashboard provides a summary view of risk and compliance data intended for senior-level security officers.

- **[Building audit processes](#)**

Use the Audit Process Builder to streamline your compliance workflow process by consolidating, in one spot, database activity monitoring tasks such as: asset discovery; vulnerability assessment and hardening; database activity monitoring and audit reporting; report distribution; sign off by key stakeholders; and escalations.

- **[Audit and Report](#)**

Guardium organizes the data it collects into a set of domains. Each domain contains a different type of information relating to a specific area of concern: data access, exceptions, policy violations, and so forth.

- **[External data correlation](#)**

This topic describes creating and managing custom tables and custom domains, for importing enterprise information to use with existing Guardium internal data.

- **[Privacy sets](#)**

A privacy set is a collection of elements that can be used to do special monitoring.

- **[Custom Alerting](#)**

Alert messages can be distributed via e-mail, SNMP, syslog, or user-written Java™ classes. The last option is referred to as custom alerting.

- **[Flat Log Process](#)**

The Flat Log option is a process to allow the Guardium appliance to log information without immediately parsing it in real time.

- **[Running database entitlement reports](#)**

Database entitlement reports provide up-to-date snapshots of database users and their required access privileges. Learn how to prepare and run these reports to validate and ensure that users have only the privileges that are needed to perform their duties.

- **[User Identification](#)**

Guardium provides several methods to identify application users, when the actual database user is not apparent from the database traffic.

- **[Value Change Auditing](#)**

The Value Change Auditing feature tracks changes to values in database tables.

- **[Creating an Audit Database](#)**

Create an audit database and perform value-change monitoring activities.

- **[Monitored Table Access](#)**

This feature adds a "Last Assessed" field to relevant tables, for interaction with Optim Designer data lifecycle products.

- **[Installing and activating the FamMonitor on Windows servers](#)**

The FamMonitor enables monitoring and collection of audit information and policy rules, and real time alerts or blocking of suspicious users or connections on your Windows servers. You can install it by command line, the wizard, or GIM.

- **[File Activity Monitor for NAS and SharePoint](#)**

The Guardium File Activity Monitor (FAM) monitors activity across files and directories residing on NAS devices and SharePoint servers in the Windows environment.

- **[How to use PCI/DSS Accelerator to implement PCI compliance](#)**

Configure IBM® Guardium's PCI/DSS Accelerator and create a series of policies and reports, in order to meet PCI/DSS requirements.

- [Workflow Builder](#)

Use the Workflow Builder to define customized workflows (steps, transitions, and actions) that you can use with audit processes.

## Enabling and disabling the Investigation Dashboard

This topic describes how to enable and disable the Investigation Dashboard.

### Before you begin

The Investigation Dashboard has following minimum hardware requirements:

- 64-bit architecture
- 24 GB RAM
- 4-core CPU
- Investigation Dashboard functionality opens ports 8983 and 9983 on both central managers and collectors. The ports are opened when the Investigation Dashboard is enabled and closed when it is disabled. To use the Investigation Dashboard, ensure that bidirectional communication between Central managers and collectors on ports 8983 and 9983 is not blocked by any firewall.
- Central managers and managed units must be able to reach each other via host name and IP address: ensure that DNS is configured to resolve IP addresses and host names in both forward and reverse lookup. If DNS cannot be used, use the **support store hosts** command to manually add IP-host name combinations. For more information, see [support store hosts](#).

Restriction: The Investigation Dashboard and Data Level Security cannot be enabled concurrently.

### Procedure

1. Log in to the Guardium® system as a user or administrator with the CLI role.
2. Enable the Investigation Dashboard with the GuardAPI command:

```
grdapi enable_quick_search schedule_interval=2 schedule_units=MINUTE
```

To enable the Investigation Dashboard on all managed units of an environment, use the all=true parameter:

```
grdapi enable_quick_search schedule_interval=2 schedule_units=MINUTE all=true
```

Note: This GuardAPI executes many configuration scripts and, depending on the current unit status, can take a few minutes. By default, violations are not included in search results. To include violations, set the includeViolations parameter to **true**:

```
grdapi enable_quick_search schedule_interval=2 schedule_units=MINUTE includeViolations=true
```

To enable outlier detection, see [Outliers detection](#).

Additional parameters may be specified, such as the search index update interval. For more information, see [Investigation Dashboard APIs](#).

3. Use the following GuardAPI command to disable the Investigation Dashboard function at any time:

```
grdapi disable_quick_search
```

### Results

After you have enabled the Investigation Dashboard, see [Accessing the investigation dashboard](#) to learn more and begin using the investigation dashboard.

Attention: Indexed search data is retained for 3 days. Use the purge object Guardium CLI command to change the retention period. For example, the following command changes the retention period to 5 days: **store purge object age 36 5**. Note that 36 is the default object identification number associated with the search index. For additional information, see [Configuration and Control CLI Commands](#) reference information.

### Related reference

- [Investigation dashboard APIs](#)
- [Investigation dashboard CLI commands](#)

### Related information

- [Troubleshooting: Investigation dashboard is not showing results](#)

## Basic data security monitoring policy

Use the basic data security monitoring policy to get started with Guardium SQL traffic monitoring.

Guardium ships with a pre-defined policy installed by default: Default - Ignore Data Activity for Unknown Connections [template]. This default captures session-level information such as client and server IP addresses, database type, operating system user, source program, and database session start and end times, but it does not capture actual SQL activity.

Compared to the default policy, the basic data security monitoring policy allows you to starting monitoring SQL traffic right out of box. Using predefined groups of privileged users, privileged commands, and error codes for some of the most common use cases, the basic monitoring policy provides rules that address common data

access and attack patterns. Although it is not a comprehensive auditing policy, the basic monitoring policy offers a secure foundation while you develop database activity monitoring policies specific to your environment and needs.

#### 1. Prerequisites for the basic data security monitoring policy

Take simple steps to verify that you are ready to begin using the basic data security monitoring policy.

#### 2. Install the basic data security monitoring policy

#### 3. Create reports for basic data security monitoring

Create reports for monitoring administrative user activity and command execution.

#### 4. Next steps for data security monitoring

After installing the basic data security monitoring policy and creating reports, begin tuning the policies and using advanced analytics.

---

## Prerequisites for the basic data security monitoring policy

Take simple steps to verify that you are ready to begin using the basic data security monitoring policy.

## Procedure

---

### 1. Install S-TAP monitoring agents on your database servers and confirm that the S-TAP inspection engines are correctly configured.

For information about installing S-TAPs using the Guardium Installation Manager (GIM), see [Deploy monitoring agents](#). View or modify inspection engines on collectors by navigating to [Manage > Activity Monitoring > S-TAP Control](#).

### 2. Verify that S-TAPs are not configured to ignore database responses.

The db\_ignore\_response configuration parameter in the S-TAP configuration file guard\_tap.ini should be set to none (the default value). If you are managing the S-TAP using GIM, the equivalent GIM parameter is STAP\_DB\_IGNORE\_RESPONSE for Linux and UNIX systems or WINSTAP\_DB\_IGNORE\_RESPONSE for Windows systems.

### 3. Verify that the Log Records Affected setting is enabled for the inspection engines.

On each collector in a standalone environment (no central manager), navigate to [Manage > Activity Monitoring > Inspection Engines](#), select the Log Records Affected check box, and click Apply. Alternatively, log in to the each collector via SSH as the cli user and run the following command: `grdapapi update_engine_config logRecords=true`

In a managed environment, log in to the central manager via SSH as the cli user and run the following command once for each managed collector host name: `grdapapi update_engine_config logRecords=true api_target_host=<managed collector host name>"`

### 4. Upload the latest Guardium Database Protection Subscription Service (DPS) update to each collector in a standalone environment or to the central manager in a managed environment.

The latest DPS update is available on IBM Fix Central.

- Navigate to [Harden > Vulnerability Assessment > Customer Uploads](#).
- In the DPS Upload section, click Browse and choose the latest DPS update file, then click Upload.
- In the Import DPS section, click on the  icon to import the DPS update.

The import may take a while to finish. You can monitor the status of the import by connecting to the Guardium system via SSH as the cli user and running the following command: `show dps`

---

## What to do next

You are ready to install the basic data security monitoring policy.

Next topic: [Install the basic data security monitoring policy](#).

---

## Install the basic data security monitoring policy

## Before you begin

---

In a standalone environment (no central manager), follow this procedure on each collector. In a managed environment, follow this procedure on the central manager. For a rule-by-rule description of the basic data security monitoring policy, see [Understand the basic data security monitoring policy rules](#).

## Procedure

---

### 1. Navigate to [Protect > Security Policies > Policy Builder for Data](#).

### 2. Select the Basic Data Security Policy [template] and click [Install > Install](#).

### 3. Policy templates are cloned before installation: use the Clone policy template dialog to provide a unique name for the cloned policy and click OK.

### 4. After successful installation, click OK on the confirmation dialog.

### 5. Take the following actions on the Install policy dialog:

- Use the Installation action menu and select Install and override.  
Attention: The Install and override action replaces any currently-installed policies. Select a different installation action if you need to preserve installed policies.
- Accept the default setting to install and override All policies.
- Optional: If working from a central manager, select the managed units where the policy will be installed.
- Click OK.

---

## What to do next

Create reports based on SQL traffic collected by the basic monitoring policy.

## Understand the basic data security monitoring policy rules

Review a rule-by-rule description of the basic data security monitoring policy.

To see the rules included with the basic data security monitoring policy:

1. Go to Protect > Security Policies > Policy Builder for Data.
2. Select the Basic Data Security Policy [template] and click .
3. In the View Policy dialog, click the Rules section. The policy rules and criteria are listed in the table.

### Rule 1: XSS

This rule uses regular expression to detect well-known XSS (cross-site scripting) attack patterns in the SQL. Such code, if stored in the database, can be used to attack the WEB-UI. The rule action generates a high severity policy violation.

### Rule 2: SQL injection - tautology

This rule uses regular expression to detect a common pattern of SQL injection attack. Expressions such as `1=1` can be used by an attacker to add arbitrary SQL code at the end of improperly formed statements. The rule action generates a high severity policy violation.

### Rule 3: SQL injection - denial of service (DoS)

This rule uses regular expression to detect a common pattern of SQL injection attack. Commands such as `benchmark` can be used by an attacker to overload the database. The rule action generates a high severity policy violation.

### Rule 4: SQL injection - side channel

This rule uses regular expression to detect a common pattern of SQL injection attack. The `sleep` command, when embedded in SQL, can create performance and timeout issues and fail applications. The rule action generates a high severity policy violation.

### Rule 5: OS command injection

This rule uses regular expression to detect OS commands and executable code in SQL. Such code, if stored in the database, can be used to attack back-end or front-end systems. The action generates a high severity policy violation.

Rules 1-5 should be tuned to meet the specific needs of a specific environment to reduce false positives. Occurrences of each of these patterns might be an indication of an attack but they can also be legitimate actions on some environments. For example, rule 1 may generate false positives if it is applied to an application where logic intentionally uses many HTML tags in SQL statements. The rule conditions can be tuned to limit the rule to applications where many HTML tags in SQL statements are not expected, therefore SQL statements with HTML tags might indicate an XSS attack. Likewise, `1=1` and similar logic expressions (even `1=0`) are widely used in legitimate software. When these rules fire on legitimate operations they can be tuned by adding more criteria in the rules themselves, or in the policy, to distinguish between legitimate and illegitimate operations.

Note: The violations generated by rules 1 - 5 are also used by *Active Threat Analytics* if the feature is enabled.

### Rule 6: Monitor all database activity for admin users

This rule relies on the pre-defined Guardium group *Admin Users* to identify and comprehensively log all activities that are performed by those users. The rule uses the `LOG FULL DETAILS` action, and the group is per-populated with the default admin and certain non-admin users for most supported database types. The group does not contain any custom users with admin privileges that typically exist in production environments. To view admin users activity logged in Guardium, go to Reports > My Custom Reports > Admin Users Activity.

For more information, see [Create an Admin Users Activity report](#).

### Rule 7: Monitor all administrative commands

This rule relies on the pre-defined Guardium group *Administrative Commands* to identify and comprehensively log all activities that contain administrative commands that are listed in the group. The rule uses the `LOG FULL DETAILS` action, and the group is per-populated with the default administrative commands for most supported database types. To view administrative commands logged in Guardium, go to Reports > My Custom Reports > Administrative Commands Execution. For more information, see [Create an Administration Commands Execution report](#).

### Rule 8: Log a policy violation for repeated failed login attempts

This rule logs a policy violation if five or more failed login attempts are made within a 1-minute time interval. The rule uses the `LOG ONLY` action. Attempts by a malicious user to repeatedly guess the database password by trial and error might be captured by this rule. To view policy violations logged in Guardium, go to Comply > Reports > Incident Management to view the *Policy Violations / Incident Management* report. The Access Rule Description field indicates which policy rule triggered the violation.

### Rule 9: Log a policy violation if risk-indicative errors are generated

This rule relies on the predefined Guardium group *Risk-indicative error messages*. This group contains errors typically associated with malicious or unauthorized activities. The rule logs a policy violation when an error in that group occurs. The rule uses the `LOG ONLY` action. To view policy violations logged in Guardium, go to Comply > Reports > Incident Management to view the *Policy Violations / Incident Management* report. The Access Rule Description field indicates which policy rule triggered the violation.

### Rule 10: Log a policy violation on potential data exfiltration attempts

This rule inspects the number of rows that are returned by the database in response to queries per database session to identify potential *data exfiltration* attempts. Data exfiltration refers to attempts to move large amounts of data. If the total number of rows that are returned by database for a session reaches or exceeds 1000 within a 1-minute time interval, a policy violation is logged with the `LOG ONLY` action. To view policy violations logged in Guardium, go to Comply > Reports > Incident Management to view the *Policy Violations / Incident Management* report. The Access Rule Description field indicates which policy rule triggered the violation.

### Rule 11: Ignore heavy traffic load sessions (typically batch jobs)

This rule is designed to filter out traffic from potentially heavy batch jobs to avoid overwhelming the Guardium collector. This rule counts the number of SQL statements that are executed within a session. If the number reaches or exceeds 500 within a 1-minute time interval, the remainder of the session is ignored by using the `IGNORE S-TAP SESSION` action. The first 500 SQL statements for that session are logged for audit purposes.

## Create reports for basic data security monitoring

Create reports for monitoring administrative user activity and command execution.

## Procedure

---

1. On each collector in a standalone environment or on the central manager in a managed environment, navigate to [Investigate > Query-Report Builder](#).
2. [Create an Admin Users Activity report](#).
3. [Create an Administration Commands Execution report](#).

Previous topic: [Install the basic data security monitoring policy](#)  
Next topic: [Next steps for data security monitoring](#)

---

## Create an Admin Users Activity report

### Procedure

---

1. In the Queries-Reports pane, use the menu to select the Access domain.
2. Click  to open the New Query builder.
3. In the Query Name section, in the Query Name field, type `Admin Users Activity`.
4. Use the Select main entity menu to select FULL SQL.
5. Click Next.
6. In the Selected Columns section, select the following *Entity: Attribute* pairs then click  to add them to the report.
  - Client/Server: Analyzed Client IP
  - Client/Server: DB User Name
  - Client/Server: Server IP
  - Client/Server: Source Program
  - Client/Server: Service Name
  - FULL SQL: Full Sql
  - FULL SQL: Timestamp
7. Click Next.
8. In the Sort Order section, accept the default Sort results by column setting and click Next.
9. In the Conditions section, click  to add the following condition: Client/Server: DB User Name with the operator IN GROUP and group Admin Users.
10. Click Save.
11. Click Add to My Custom Reports to add the report to the [Reports > My Custom Reports](#) navigation item.

## Create an Administration Commands Execution report

### Procedure

---

1. In the Queries-Reports pane, use the menu to select the Access domain.
2. Click  to open the New Query builder.
3. In the Query Name section, in the Query Name field, type `Administration Commands Execution`.
4. Use the Select main entity menu to select FULL SQL.
5. Click Next.
6. In the Selected Columns section, select the following *Entity: Attribute* pairs then click  to add them to the report.
  - Client/Server: Analyzed Client IP
  - Client/Server: DB User Name
  - Client/Server: Server IP
  - Client/Server: Source Program
  - Client/Server: Service Name
  - FULL SQL: Full Sql
  - FULL SQL: Timestamp
7. Click Next.
8. In the Sort Order section, accept the default Sort results by column setting and click Next.
9. In the Conditions section, click  to add the following condition: Command: SQL Verb with the operator IN GROUP and group Administrative Commands.
10. Click Save.
11. Click Add to My Custom Reports to add the report to the [Reports > My Custom Reports](#) navigation item.

## Next steps for data security monitoring

After installing the basic data security monitoring policy and creating reports, begin tuning the policies and using advanced analytics.

### Procedure

---

1. Using the `Admin Users Activity` and `Administrative Commands Execution` reports, examine the traffic to identify and ignore trusted sessions. For more information, see the following videos:
  - [Guardium Policies: Part 1: Logging behavior and introduction to constructs](#)
  - [Guardium Policies: Part 2: Using policies to change logging behavior - Log full details](#)
  - [Guardium Policies: Part 3: Using policies to change logging behavior - Ignore Sessions](#)

- [Guardium Policies: Part 4: Using policies to change logging behavior - Alerting rules](#)
2. Run advanced analytics on the data logged by the *basic data security monitoring policy*.  
To learn more about enabling and using advanced analytics, see the following information:
  - [Active Threat Analytics](#)
  - [Outliers detection](#)
  - [Risk Spotter](#)
3. Continuously monitor and tune policies to keep up with the changes in the database and application landscape.  
The *basic data security monitoring policy* provides a starting point for monitoring and analyzing traffic, but your organization needs to maintain and tune policies according to the observed traffic and organizational requirements.

Previous topic: [Create reports for basic data security monitoring](#)

---

## Smart assistant for compliance monitoring

The compliance monitoring smart assistant helps you quickly configure monitoring for GDPR, PCI, SOX, and other security standards and regulations.

To get started, navigate to [Setup > Smart Assistant > Compliance Monitoring](#) and click the Set up compliance monitoring tile to begin. For more information about using the smart assistant, see [Set up compliance monitoring or application data monitoring](#).

Templates are provided to support the following standards and regulations:

- Basel Committee on Banking Supervision (BASEL II)
- California Consumer Privacy Act (CCPA)
- General Data Protection Regulation (GDPR)
- General Data Protection Regulation for Db2 for z/OS (GDPR for Db2 for z/OS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Security Standard (PCI)
- Personally Identifiable Information (PII)
- Sarbanes-Oxley Compliance (SOX)
- **Databases**  
Use the database tab of the compliance monitoring smart assistant to identify databases for monitoring and manage database credentials needed for discovering sensitive data.
- **Applications**  
The applications tab of the compliance monitoring smart assistant provides a tree-based view of all applications and their assigned databases.
- **Compliance summary**  
The compliance summary provides an at-a-glance view of compliance monitoring configuration and immediate access to related policies, groups, and reports.
- **Application summary**  
The application summary provides an immediate view of database monitoring, group population, and policies associated with an application, including key security metrics for the associated databases.
- **Set up compliance monitoring or application data monitoring**  
The compliance and application data monitoring wizard is provided to automate many of the actions involved with policy configuration and deployment.

## Related concepts

---

- [Policies](#)
- [Groups](#)
- [Datasources](#)

## Related tasks

---

- [Discover Sensitive Data](#)
- 

## Databases

Use the database tab of the compliance monitoring smart assistant to identify databases for monitoring and manage database credentials needed for discovering sensitive data.

Identifying databases in your environment that require data protection is an important part of configuring compliance monitoring. The databases tab of the compliance monitoring smart assistant displays an inventory of known databases and a summary of their configuration status. Use this inventory to track compliance monitoring configuration status, add databases for monitoring, and manage the database credentials used for discovering sensitive data.

The database inventory supports the following database types:

- Db2
- Db2 z/OS
- Informix
- MongoDB
- MS SQL Server
- MS SQL SERVER (DataDirect)
- MS SQL SERVER (DataDirect - Dynamic Port)
- MySQL
- Netezza
- Oracle
- Oracle (DataDirect - Service Name)

- Oracle (DataDirect - SID)
- PostgreSQL
- SAP HANA
- Sybase
- Sybase IQ
- Teradata

Note: The inventory of known databases is established by any of the following:

- Observed traffic on collectors
- Existing datasources on a central manager
- Databases added using the compliance monitoring or database inventory tools, for example Import from CSV and Reconcile assets.

Known databases are refreshed hourly and the data is retained for 30 days by default.

It is possible to have more datasources defined than databases in the inventory. This happens when the same database is used in multiple datasource definitions or when a database that is not supported by the inventory is used in a datasource definition.

Get started by adding databases to the inventory. From the Databases tab, click the  icon to add an individual database or click the Import from CSV button to import multiple databases.

- [Add an individual database](#)  
Add an individual database to the inventory by manually providing information such as database type, host name, and service name.
- [Import multiple databases](#)  
Import multiple databases to the inventory from a spreadsheet containing information such as database type, host name, and service name.
- [Reconciling database inventory](#)  
Asset reconciliation compares a user-provided list of databases with the databases that are known to Guardium. This feature offers a quick way to identify old or unknown databases and to verify that Guardium provides the coverage that you want.

## Add an individual database

Add an individual database to the inventory by manually providing information such as database type, host name, and service name.

### Procedure

1. Click the  icon to open the Add database dialog.
2. Use the Database type menu to select the type of database to add.
3. The fields for defining a database vary depending on the database type. Complete all required fields.
4. Click OK to add the database.

### Results

An individual database is imported to the compliance monitoring database inventory. If you specified database credentials, the credentials are saved and a datasource is created for discovering sensitive data, running vulnerability assessments, and use with other Guardium processes. Configure advanced datasource features such as connection properties using the Setup > Tools and Views > Datasource definitions tool.

## Import multiple databases

Import multiple databases to the inventory from a spreadsheet containing information such as database type, host name, and service name.

### Before you begin

Importing databases is a quick and convenient way to populate the compliance monitoring smart assistant with databases for monitoring. Before you begin, prepare a comma-separated values (CSV) file with the database information to import. The file needs to meet the following requirements:

- The first row defines column names.
- Each row is complete, meaning that empty fields are accounted for with a delimiter (for example, a comma).
- Database type is defined using any of the following case-insensitive strings:
  - Db2
  - Db2 z/OS
  - Informix
  - MongoDB
  - MS SQL Server
  - MS SQL SERVER (DataDirect)
  - MS SQL SERVER (DataDirect - Dynamic Port)
  - MySQL
  - Netezza
  - Oracle
  - Oracle (DataDirect - Service Name)
  - Oracle (DataDirect - SID)
  - PostgreSQL
  - SAP HANA
  - Sybase
  - Sybase IQ

- Teradata
- MS SQL Server can be used for both MS SQL SERVER (DataDirect) and MS SQL SERVER (DataDirect - Dynamic Port) databases. Oracle can be used for both Oracle (DataDirect - SID) and Oracle (DataDirect - Service Name) databases.
- All database types require values for the Host name/IP address and Port number fields. In addition, specific databases require additional fields:
    - Db2, Db2 z/OS, Netezza, and PostgreSQL require Database name.
    - Informix requires Informix server.
    - MS SQL SERVER (DataDirect - Dynamic Port) requires Instance name. Note: port number is not required for MS SQL SERVER (DataDirect - Dynamic Port).
    - Oracle (DataDirect - Service Name) and Oracle (DataDirect - SID) require Service name.

Attention: Microsoft Excel format (XLS) is not supported. When exporting CSV from Excel, verify that the CSV file is created with complete rows and is not missing delimiters for empty fields.

## Procedure

---

1. Click the Import from CSV button to open the Import from CSV dialog.
2. Click the Browse button and select a CSV file to upload.
3. Use the Field delimiter field to define the delimiter used in the CSV file.  
In most instances, the default value (a comma) is appropriate.
4. Click the Load button to continue.
5. Use the drop-down menus to map columns from the CSV file to specific database information.  
For example, to import host information, use the Host name/IP menu to select the column name containing the host names or IP address of your databases.  
Note: Columns containing Instance name, Server name, and Service name information are automatically assigned based on the associated database type. For example, in a CSV file containing Db2 instance names and Oracle service names in a single column, mapping that column to either Instance name or Service name fields assigns the value to the correct field for the database type.
6. Click OK to import database information from the CSV file.  
If needed, a warning message displays any rows that are skipped due to incomplete or invalid data.

## Results

---

Multiple databases are imported to the compliance monitoring database inventory. If you imported database credentials, the credentials are saved and datasources are created for discovering sensitive data, running vulnerability assessments, and use with other Guardium processes. Configure advanced datasource features such as connection properties using the Setup > Tools and Views > Datasource definitions tool.

## Reconciling database inventory

---

Asset reconciliation compares a user-provided list of databases with the databases that are known to Guardium. This feature offers a quick way to identify old or unknown databases and to verify that Guardium provides the coverage that you want.

### Before you begin

---

Asset reconciliation supports the following databases:

- Db2
- Db2 z/OS
- Informix
- MongoDB
- MS SQL Server
- MS SQL SERVER (DataDirect)
- MS SQL SERVER (DataDirect - Dynamic Port)
- MySQL
- Netezza
- Oracle
- Oracle (DataDirect - Service Name)
- Oracle (DataDirect - SID)
- PostgreSQL
- SAP HANA
- Sybase
- Sybase IQ
- Teradata

Unsupported databases cannot be reconciled and are ignored with an error message.

Attention: Microsoft Excel format (XLS) is not supported. When exporting CSV from Excel, verify that the CSV file is created with complete rows and is not missing delimiters for empty fields.

## About this task

---

Reconciling database inventory (asset reconciliation) compares databases that are known to Guardium with an external, user-provided list of databases. Asset reconciliation accepts CSV or CMDB inputs and categorizes databases as existing only in Guardium, only in the external list, or as existing in both Guardium and the external list. For databases that are known to Guardium, the reconciliation process shows information about where the database is used, for example, in a datasource definition or with compliance monitoring. Asset reconciliation also supports an allowlist of databases that are not known to Guardium that can be ignored in the future.

## Procedure

---

1. Browse to Setup > Smart Assistant > Compliance Monitoring.
2. Select the Databases tab and click Reconcile assets to open the Reconcile database inventory dialog.
3. Select the list of databases to compare with databases that are known to Guardium.
  - To use a CSV file, select Compare to CSV file.
    - a. Click Browse and select a CSV file that contains the list of databases to compare.
    - b. Click Load to begin working with the CSV file.
    - c. Use the drop-down menus to map columns from the CSV file to specific database information.  
For example, to map host information, use the Host name/IP menu to select the column name that contains the hostnames or IP address of your databases.

Note:

    - Database type is a required field and must match one of the supported databases. For example, the strings Db2 LUW or Db2 v11 do not match the expected value, Db2.
    - Columns containing Instance name, Server name, and Service name information are automatically assigned based on the associated database type.  
For example, in a CSV file that contains Db2 instance names and Oracle service names in a single column, mapping that column to either Instance name or Service name fields assigns the value to the correct field for the database type.
  - d. Click OK.
  - To use CMDB, select Compare to CMDB.
    - a. Select an existing CMDB URL or click to add a new one.  
To add a new URL, define the Type (for example, Service Now), URL from the CMDB provider, and account credentials.
    - b. Select a Table to reconcile.
    - c. Click Load to begin working with the CMDB records.
    - d. Use the drop-down menus to map fields from the CMDB records to specific database information.  
For example, to map host information, use the Host name/IP menu to select the column name that contains the hostnames or IP address of your databases.

Note: Columns that contain Instance name, Server name, and Service name information are automatically assigned based on the associated database type.  
For example, in the CMDB table that contains Db2 instance names and Oracle service names in a single column, mapping that column to either Instance name or Service name fields assigns the value to the correct field for the database type.
  - e. Click Run Now or Schedule.
4. Begin working with the Asset reconciliation results dialog.

#### Databases not in Guardium

This table shows databases that are listed in the input (either CSV or CMDB) that are not known to Guardium.

- Select databases and click Add to allowlist to prevent them from appearing in this table during future reconciliations. You are asked to provide a brief justification for adding the databases to the allowlist.
- Select databases and click Add to Guardium inventory to add them to Guardium's list of known databases. After the databases are added to the inventory, they are available for use with compliance monitoring and other features.

#### Databases only in Guardium

This table shows databases that are known to Guardium but not listed in the input. In addition, the table indicates whether Guardium has observed traffic on the databases and how the databases are used in Guardium (for example in datasource definitions or compliance monitoring).

- Select databases and click to remove them from the Guardium list of known databases.

#### Matched databases

This table shows databases that are listed in the input and that are also known to Guardium. In addition, the table indicates whether Guardium has observed traffic on the databases and how the databases are used in Guardium (for example, in datasource definitions or compliance monitoring).

#### Rows rejected

This table lists rows from the input that identify an unsupported database type or do not contain enough information to uniquely identify a database. Each entry contains a brief description of the problem with the input.

#### Allowlist databases

This table lists databases in the input that can be ignored during the reconciliation process.

## Related information

- [IBM Guardium Security V11.2 Asset reconciliation video](#)

## Applications

The applications tab of the compliance monitoring smart assistant provides a tree-based view of all applications and their assigned databases.

Use the applications tab to create, update, and delete applications. It is also possible to import a list of applications from CSV.

- [Add an individual application](#)  
Add an individual application for compliance monitoring and assign databases to the application.
- [Import multiple applications](#)  
Import multiple applications and industries from a spreadsheet.

## Add an individual application

Add an individual application for compliance monitoring and assign databases to the application.

## Procedure

1. Navigate to Setup > Smart Assistant > Compliance Monitoring and select the Applications tab.
2. Click the icon to open the New application dialog.
3. Optional: Use the Industry menu to select a predefined industry. Otherwise, type to define a new industry name.  
Selecting a predefined industry filters the Application menu.

Use the Industry field to define a meaningful hierarchy of applications in your environment. For example, create industries to group applications by geographical region such as Customer Relationship Management (North America) and Customer Relationship Management (Europe) or to separate Production and Test applications.

4. Use the Application menu to select an existing application. Otherwise, type to define a new application name.
5. Use the check boxes to select databases and the  and  icons to assign databases to the application.  
Databases added to the table using the  icon are assigned to the application.
6. Click Save to add the application and its assigned databases to the table.

## Results

---

An application is added to the table. If specified, the industry name is displayed in parentheses after the application name. View the databases assigned to an application by clicking the  icon next to the application name.

## What to do next

---

Edit existing applications using the  icon. Remove applications using the  icon.

Applications that have not been configured for compliance monitoring display an  icon in the Unconfigured column. To set up compliance monitoring for an application, use the Application summary tab and click the  icon for Set up application data monitoring.

---

## Import multiple applications

Import multiple applications and industries from a spreadsheet.

## Before you begin

---

Importing applications and industries is a quick and convenient way to populate the compliance monitoring smart assistant with applications for monitoring. Before you begin, prepare a comma-separated values (CSV) file with the information to import. The file needs to meet the following requirements:

- The first row defines column names.
- Each row is complete, meaning that empty fields are accounted for with a delimiter (for example, a comma).

Attention: Microsoft Excel format (XLS) is not supported. When exporting CSV from Excel, verify that the CSV file is created with complete rows and is not missing delimiters for empty fields.

## Procedure

---

1. Navigate to Setup > Smart Assistant > Compliance Monitoring and select the Applications tab.
2. Click the Import from CSV button to open the Import from CSV dialog.
3. Click the Browse button and select a CSV file to upload.
4. Use the Field delimiter field to define the delimiter used in the CSV file.  
In most instances, the default value (a comma) is appropriate.
5. Click the Load button to continue.
6. Use the drop-down menus for Application name and Industry name to map columns from the CSV file to application and industry names.  
Use the Industry field to define a meaningful hierarchy of applications in your environment. For example, create industries to group applications by geographical region such as Customer Relationship Management (North America) and Customer Relationship Management (Europe) or to separate Production and Test applications.
7. Click OK to import application information from the CSV file.  
If needed, a warning message displays any rows that are skipped due to incomplete or invalid data.

## Results

---

Multiple applications are imported to the table. If specified, industry names are displayed in parentheses after the application names.

## Compliance summary

---

The compliance summary provides an at-a-glance view of compliance monitoring configuration and immediate access to related policies, groups, and reports.

Open the summary by navigating to Setup > Smart Assistant > Compliance Monitoring and clicking the Compliance summary tab.

To configure a new compliance monitoring type, click the  icon on the Set up compliance monitoring tile. For more information about using the compliance monitoring wizard, see [Set up compliance monitoring or application data monitoring](#).

Several actions are available for configured compliance types:

- Click the View details link to open a panel showing associated groups, databases, policies, and reports. Tabs on the details panel provide convenient links for populating groups, opening tools like the Policy builder for data, or viewing reports.
- Click the  icon to open the compliance monitoring wizard and make changes to an existing configuration.

## Application summary

The application summary provides an immediate view of database monitoring, group population, and policies associated with an application, including key security metrics for the associated databases.

Open the summary by navigating to [Setup > Smart Assistant > Compliance Monitoring](#) and clicking the Application summary tab.

To configure a new application for data monitoring, click the  icon on the Set up application data monitoring tile. For more information about using the compliance monitoring wizard, see [Set up compliance monitoring or application data monitoring](#).

Several actions are available for configured applications:

- Click the View details link to open a panel showing associated groups, databases, policies, and reports. Tabs on the details panel provide convenient links for populating groups, opening tools like the Policy builder for data, or viewing reports.
- Click the  icon to open the compliance monitoring wizard and make changes to an existing application.

## Set up compliance monitoring or application data monitoring

The compliance and application data monitoring wizard is provided to automate many of the actions involved with policy configuration and deployment.

The wizard automates the following actions:

- A security policy is created and installed for the selected compliance type.
- A policy installation schedule is defined for 10:30 AM daily.
- A server IP group is populated with the server IP addresses of the selected databases.
- The current user is assigned to the selected compliance-type role, enabling access to the related reports and accelerators.
- Optionally create a discovery scenario for identifying and classifying sensitive data.
- Provide a summary of actions taken and next steps to finish configuring compliance monitoring.

Open the compliance and application data monitoring wizard by navigating to [Setup > Smart Assistant > Compliance monitoring](#) and selecting either the Compliance summary tab or the Application summary tab. Click the  icon to configure a new compliance type or the  icon to edit an existing configuration.

Note: Complete the compliance and application data monitoring wizard for each compliance type you want to configure. For example, to configure both GDPR and PCI, complete the wizard once for GDPR and then again for PCI.

### 1. Prerequisites for the compliance and application data monitoring smart assistant

The compliance and application data monitoring wizard has two optional prerequisites: deploying monitoring agents (S-TAPs) to database servers and gathering database credentials to allow Guardium to scan for tables containing sensitive data. Either of these steps can be completed later.

### 2. Select compliance type

Select one of the supported compliance types to configure, for example GDPR, PCI, or SOX, or configure monitoring using a custom policy.

### 3. Select databases or applications to monitor

Select known databases and applications for monitoring, or add information about new databases and applications.

### 4. Search for sensitive data

Identify database tables that contain sensitive data and add those tables to groups for monitoring.

### 5. Summary

See an overview of compliance and application data monitoring wizard actions and actions that you must take to complete the configuration. The summary is based on your progress through the wizard and configuration you may have completed elsewhere in Guardium.

## Prerequisites for the compliance and application data monitoring smart assistant

The compliance and application data monitoring wizard has two optional prerequisites: deploying monitoring agents (S-TAPs) to database servers and gathering database credentials to allow Guardium to scan for tables containing sensitive data. Either of these steps can be completed later.

## Before you begin

Open the compliance and application data monitoring wizard by navigating to [Setup > Smart Assistant > Compliance monitoring](#) and selecting either the Compliance summary tab or the Application summary tab. Click the  icon to configure a new compliance type or the  icon to edit an existing configuration.

## Procedure

### 1. From the Before you begin section, review the notes and prerequisites.

- Monitoring agents (S-TAPs) must be installed on database servers in order to monitor data. The agents do not need to be installed before completing the compliance monitoring configuration, but monitoring will not actually begin until the agents are installed.
- Use [Setup > Tools and Views > Configure Universal Connector](#) to establish monitoring with universal connectors. Universal connectors appear in Compliance Monitoring only after they have active traffic.
- Guardium needs appropriate database credentials to scan for and discover database tables containing sensitive data. If you want to configure discovery at this time, you will need to have the database credentials ready. Otherwise, credentials can be supplied later.

### 2. Click the Next button to continue.

**Next topic:** [Select compliance type](#)

## Select compliance type

Select one of the supported compliance types to configure, for example GDPR, PCI, or SOX, or configure monitoring using a custom policy.

### Procedure

- From the Select compliance type section, use the Which compliance type do you want to configure? control to select either Out of the box policies or Custom policies.  
Out of the box policies are predefined policies that support established data-security standards. For example, to configure the payment card industry standard, select Payment Card Industry Data Security Standard (PCI). Custom policies are policies you have created or modified outside the compliance and application data monitoring wizard, for example using the Policy Builder for Data.
- Click Next to continue through the wizard or click any of the enabled sections to edit its configuration.

**Previous topic:** [Prerequisites for the compliance and application data monitoring smart assistant](#)

**Next topic:** [Select databases or applications to monitor](#)

## Select databases or applications to monitor

Select known databases and applications for monitoring, or add information about new databases and applications.

### Procedure

- From the Select databases to monitor section:
  - Click the Databases tab and use the check boxes to select one or more databases for monitoring.  
If you have not previously added databases to the inventory, add individual databases by clicking the icon or import information about multiple databases by clicking the Import from CSV button. For more information, see:
    - [Add an individual database](#)
    - [Import multiple databases](#)
  - Click the Applications tab and use the check boxes to select one or more applications for monitoring.  
If you have not previously added applications, add an application by clicking the icon or import information about multiple applications by clicking the Import from CSV button. For more information, see:
    - [Add an individual application](#)
    - [Import multiple applications](#)

It is possible to select both databases and applications for monitoring.

- Click Next to continue through the wizard or click any of the enabled sections to edit its configuration.

**Previous topic:** [Select compliance type](#)

**Next topic:** [Search for sensitive data](#)

## Search for sensitive data

Identify database tables that contain sensitive data and add those tables to groups for monitoring.

### Procedure

- From the Search for sensitive data section, choose one option for identifying sensitive data.
  - The Scan for tables option uses the Guardium classifier to discover tables containing sensitive objects in your databases. The classifier requires credentials with adequate database privileges to perform the scan.
    - Use check boxes to select databases. Databases that are ready for scanning show a icon in the Ready for classification column. If needed, use the Add credentials link to specify login credentials for scanning a selected database.
    - Click Test connection to verify that the supplied credentials are valid for the databases being tested. The connection test does not verify that the supplied credentials have adequate database privileges to perform the classification scan.
  - If you already know where the sensitive data is located in your databases, select Manually define table names to manually define the table names or import a CSV file containing a list of table names that contain sensitive data.
    - Click the Browse button and identify a comma separated value (CSV) file containing sensitive objects.
    - Set the Field delimiter value to the separator used in the CSV file. The default value is a comma (,).
    - The Column to import menu displays columns from the selected CSV file. Use the menu to select the column containing sensitive object.
    - Click the Load button to add the sensitive objects to the Member table. Repeat the previous steps to import multiple columns or multiple CSV files.
    - In the Member table, add items by clicking the icon or remove items by selecting items and clicking the icon.
  - The Skip for now option allows you to identify the sensitive data in your databases at a later time. However, compliance monitoring policies depend on knowing where to look for sensitive objects, and your compliance monitoring strategy will not be complete until you complete this step. Return to the Search for sensitive data section at any time to complete this configuration.

Attention: When working with custom policies, Skip for now is the only available option. Use the Discover Sensitive Data tool to search for sensitive data on systems monitored with custom policies.

- Click Next to continue through the wizard or click any of the enabled sections to edit its configuration.

**Previous topic:** [Select databases or applications to monitor](#)

**Next topic:** [Summary](#)

## Summary

See an overview of compliance and application data monitoring wizard actions and actions that you must take to complete the configuration. The summary is based on your progress through the wizard and configuration you may have completed elsewhere in Guardium.

## Procedure

1. From the Summary section, review actions listed under Clicking Run setup takes the following actions.  
In particular, note the following:
  - Install compliance monitoring policy: click the View details link to view the policy and its rules.
  - Schedule policy re-installation: click the Edit link to view and edit the policy installation schedule. Regularly reinstalling policies is important if your groups are likely to change, for example when updating users or sensitive objects.
2. Review actions listed under You must complete the following actions.  
These actions are required to ensure effective compliance monitoring of your databases. In particular, note the following:
  - Populate groups: click the View details link to review and add members to groups. To add members, click the  icon next to the group to open the Edit group dialog. For more information, see [Using the group builder](#).
  - Install monitoring agents (S-TAPs) for databases: click the Install monitoring agents link to open the Smart assistant for deploying monitoring agents and begin installing S-TAPs on your database servers. For more information, see [Deploy monitoring agents](#).  
Attention: Monitoring agents are not required to complete the compliance and application data monitoring configuration, but they are required to allow monitoring data. Guardium will automatically begin monitoring data once the agents are installed.
3. Click Run setup to take the actions described in the Summary section.

Previous topic: [Search for sensitive data](#)

## Investigation Dashboard

The Investigation Dashboard provides powerful tools for identifying and assessing problems that might exist in your Guardium® environment. It uses either local or system-wide unfiltered data, and provides numerous filter options to query data across an entire Guardium environment, potentially from any Guardium collector within that environment.

The Investigation Dashboard's inter-related charts help reveal patterns, anomalies, and relationships across your data. You don't need detailed knowledge of topology, aggregation, or load balancing schemes. The Investigation Dashboard contains the original quick search for enterprise functions, and additional tools for visualizing and analyzing data.

Note: It is recommended to view the Investigation Dashboard in full screen mode.

Restriction: The Investigation Dashboard and the Data Level Security cannot be enabled concurrently.

## Operating Modes

The Investigation Dashboard supports three operating modes:

Central Manager only

Queries are submitted on a Central Manager return enterprise-wide results from all Guardium collectors with search enabled. Queries that are submitted on managed units return local results.

Central Manager only is the default operating mode.

All machines

Enterprise-wide search queries are submitted from any machine in the Guardium environment with search enabled. This mode can result in slower search results and requires connectivity between all managed units in the environment.

Local only

This mode limits search queries to the local collector where the search is submitted: no data is retrieved from other collectors in the Guardium environment. On a CM on local only mode, there is no data displayed.

See [Investigation Dashboard APIs](#) for information about setting the search mode.

- [Enabling File Activity in the investigation dashboard](#)
- [Accessing the investigation dashboard](#)
- [Using the Sankey chart](#)

The Sankey chart is an extremely useful method of investigating filtered data, for example, of a specific alert, outlier, report, or threat. Use the Sankey chart to reveal unsuspected relationships or oddities.

- [Using Data In-Sight](#)

The Data In-Sight visualization enables the user to profoundly examine a sequence of events that are captured by the Guardium system. It provides a comprehensive picture of activity in a specific time window, and helps to detect unusual behaviors.

- [Investigation Dashboard for files](#)

The investigation dashboard is a preset group of charts and a table that help you understand what is happening in your system at any given time, and upon which you can build your own customized dashboards.

- [Filtering data and saving filters in the investigation dashboard](#)

- [Filtering an individual chart](#)

You can filter an individual chart. The  icon becomes red when specific filters are set for a chart that are different than the general dashboard filters. Hover over the icon to see which filters are used in that chart.

- [Creating, saving, and exporting investigation dashboards](#)

- [Using the topology view](#)

The topology view is visualization of the Guardium appliances in the search results.

- [Local and distributed search](#)
- [Monitoring and automatic recovery for the Investigation Dashboard](#)  
Use Monitoring and automatic recovery to identify and recover issues in the investigation dashboard.

## Related reference

---

- [Investigation Dashboard APIs](#)
- [Investigation Dashboard CLI Commands](#)

## Related information

---

- [Troubleshooting: Investigation dashboard is not showing results](#)

# Enabling File Activity in the investigation dashboard

## Before you begin

---

- UNIX-Linux: S-TAP for FAM and the FAM bundle must be installed and configured.
- Windows: The FAM discovery agent and the FamMonitor must be installed and configured.
- The Investigation Dashboard must be enabled.

## About this task

---

Note: The FAM queries the server for the server IP addresses and takes the first one it finds. There is no way to select "the appropriate" IP address from a host name when the host has multiple IP addresses. Specify the IP address explicitly if you want to see that IP address in the reports.

## Procedure

---

1. On the collector, at the CLI prompt, run the GuardAPI command:

```
grdapicl enable_fam_crawler [extraction_start] [schedule_start] [activity_schedule_interval] [activity_schedule_units]
[entitlement_schedule_interval] [entitlement_schedule_units]
```

Example: The following command sends updated discovery and classification results to enterprise search for classification data every 2 minutes and for entitlement information every day.

```
grdapicl enable_fam_crawler activity_schedule_interval=2 activity_schedule_units=MINUTE entitlement_schedule_interval=1
entitlement_schedule_units=DAY
```

By default, the extraction starts when you enter the command, extracting data from the moment (time) you entered the command.

2. Repeat on each collector.

## Related concepts

---

- [File discovery and classification GIM parameters](#)
- [Investigation Dashboard for files](#)
- [Outliers detection](#)

## Related tasks

---

- [Installing and activating the FamMonitor on Windows servers](#)
- [Installing and activating FAM discovery agent \(crawler\) on Windows servers](#)
- [Installing and activating the FAM discovery agent \(crawler\) on UNIX servers](#)
- [Enabling and disabling the Investigation Dashboard](#)

## Related reference

---

- [Investigation dashboard APIs](#)

# Accessing the investigation dashboard

## Procedure

---

1. Click Investigate > Search for Data Activity or Investigate > Search for File Activity.
2. Alternatively, toggle the search to User Interface and search for investigation dashboard. Then, select either Search for Data Activity or Search for File Activity.

## Results

---

The default investigation dashboard for data or files opens. By default, the only filter that is applied to the entire dashboard is to show the last hour of data.

## Using the Sankey chart

The Sankey chart is an extremely useful method of investigating filtered data, for example, of a specific alert, outlier, report, or threat. Use the Sankey chart to reveal unsuspected relationships or oddities.

### About this task

The Sankey chart simplifies answering questions such as:

- Is a specific database getting accessed by DB users with unique IPs?
- Are all the users accessing the database with the same source programs? How many of the users exhibit unusual (exceptional) behavior?
- What is the relationship between client IP, client host name, and DB user in the specific data environment?

Advantages of the Sankey chart include:

- Presents four dimensions (and their relationships) in one view, giving a more complete and fluid view of the data that otherwise requires multiple charts.
- Provides immediate and fluent focusing and scanning by hovering over different elements (for example, DB users) and viewing all the relevant activity. The width of the related links update proportionately to the hovered link width, representing the activity flow and quantity.
- Uses line widths to intuitively reflect volumes of activity.
- Reflects, at a glance, the relationships between the selected dimensions.
- Supports the central manager level (all collectors/aggregators within one central manager).
- All fields are configurable.

### Procedure

1. In the Investigation Dashboard window, click Add Chart Data in-Sight chart. The Sankey Settings window opens.
2. Select a category, one of: Activities, Errors, Outlier details, Outlier summary, Violations. The four axis fields update accordingly.
3. Select a value for each axis field.
4. Optional: Update the MaxRows. This limits the number of objects that can be included in each axis. (Default=20.)
5. Click Save.
6. View entities by:
  - Hover over different elements (for example, DB users) to view all the relevant activity.
  - Hover over a node to get the activity flow.
  - Click a node to filter (rerender) the chart.
  - Apply filters from the facet list for deeper investigations.
7. To modify chart settings, click .

## Using Data In-Sight

The Data In-Sight visualization enables the user to profoundly examine a sequence of events that are captured by the Guardium system. It provides a comprehensive picture of activity in a specific time window, and helps to detect unusual behaviors.

### About this task

Data in-sight introduces a revolutionary paradigm that uses human visual capabilities to gain an overall view on data transactions and identify unexpected behaviors. Guardium already provides robust machine learning and data-analysis features to assist audits and detect attacks. Algorithms, data analysis, and charts are designed based on accumulated experience and knowledge. Data in-sight uses the flexibility of human vision perception to spot associations and movements in the raw data that does not fit a pattern of known attacks that would otherwise be unnoticed. The tool presents various aspects of the data in a complex visual scenario, and provides the observer with tools to directly explore large amounts of complex data.

Data in-sight converts audited data to a 3-D chronological visualization of data flow, from sources to destinations, showing data transactions unfold exactly as they occurred.

The visualization space contains two planes, each represents entities of the audit domain of a specific type. Every entry in the audit data is represented as a moving 'flash line' from an object of the upper plane (for example, client IPs) to an object of the lower plane (for example, databases). The flash line between the source and the destination leaves a trail (a dotted line) indicating the presence of interaction between the specific source and destination, which gradually fades into the background. The trails form an overview of the interaction between sources and destinations in the selected time period. The size of each source and destination is relative to their level of activity. The sources are located near their destinations, and near other similar sources. The display can be modified in various ways, giving additional information or aspects on the data. You can view data in-sight with vr headsets.

Data in-sight is an answer to this constantly changing paradigm. It adds the flexibility of human visual perception to spot associations and movements in the raw data, irrespective of known attack types, that would otherwise be unnoticed.

Data in-sight converts audited data to a 3-D chronological visualization of data sources and destinations, showing data transactions unfold exactly as they occurred. The visualization space contains two planes, each represents entities of the audit domain of a one type. Each entry in the audit data is represented as a moving 'flash line' from an object of the upper plane (client IP, OS user, DB user, or source program) to an object of the lower plane (database, object, or server). The flash line between the source and the destination leaves a trail (a dotted line) indicating the presence of interaction between the specific source and destination, which gradually fades into the background. The flash line has the same color as the destination database. The trails form an overview of the interaction between sources and destinations in the selected time period. The sources are located near their destinations, and near other similar sources. The size of the destination entity is proportional to the volume of transactions relative to the other destination entities. There are many ways of modifying the display, including: color-code the top entity (color changes as data source details change), filter from the data in-sight chart, and the investigation dashboard facets. You can also view data in-sight with vr headsets.

## Procedure

- In the Investigation Dashboard window, click Add Chart > Data In-Sight chart. The Chart Settings window opens.
- In the Chart Settings pane, modify the object types that are represented in both planes, the type of data flow between them. You can optionally color-sort the entities in the top plane by a secondary criteria, providing another level of analysis. For example, if the objects of the top plane represent client IPs and you select color-sorting for source program, you can see the usage of different source programs by a specific IP client, and the usage of a common source program by different client IPs. An object whose color changes repeatedly indicates a frequent change of source program usage in a single client IP. Click Apply.

Table 1. Data In-Sight Chart Settings

| Field                         | Description and Values                                                                                       |
|-------------------------------|--------------------------------------------------------------------------------------------------------------|
| Data flow domain              | The type of data flow displayed. One of: Activities, Errors, Violations, Outliers.                           |
| Top plane entities            | The entity that is represented in the top plane. One of: Client IP, DB User, OS User, Source Program.        |
| Bottom plane entities         | The entity that is represented in the bottom plane. One of: Database, Object, Server.                        |
| Color sort top entities by    | Extra (optional) color classification of top entities by: None, Client IP, DB User, OS User, Source Program. |
| Show top plane label          | yes, no                                                                                                      |
| Show bottom plane label       | yes, no                                                                                                      |
| Max. entities in top plane    | Maximum number of entities that are shown in the top plane.                                                  |
| Max. entities in bottom plane | Maximum number of entities that are shown in the bottom plane.                                               |
| Top entities color            | Opens color palette to select color for top plane entities. Disabled if top entities are color sorted.       |
| Background color              | Opens a color palette to select color for background.                                                        |
| Planes color                  | Opens a color palette to select color for planes (one color for both planes).                                |

- Modify the display by:
  - Click the magnifier icon to enter full screen mode for more details
  - Rotate the view by holding down the left mouse button and dragging
  - Pan by holding down the right mouse button and dragging
  - Zoom in and out with the mouse wheel
- View entities by:
  - Hover over an entity to show its details in the legend
  - Click an entity to show only its data flows (other entities fade out). Click the background to exit.
  - Double-click an entity to use it as the active filter (over the entire dashboard)

5. The information pane, which is located in the upper right corner, shows the time stamp of the current displayed actions, the number of actions shown so far, and an indication of the rate of events per second. You can modify the display by:

|  |                                                 |
|--|-------------------------------------------------|
|  | Pause/restart data flow                         |
|  | Restart data flow from beginning of time period |
|  | Increase speed of data flow                     |
|  | Decrease speed of data flow                     |
|  | View from top (bird's eye)                      |
|  | View from side (default)                        |

- Use these buttons above the Control Panel as relevant:

|  |                                                        |
|--|--------------------------------------------------------|
|  | Activates full-screen mode for the Data In-Sight chart |
|  | Opens the Chart Settings                               |
|  | Closes the Data In-Sight chart                         |
|  | Opens a pop-up help                                    |

## Investigation Dashboard for files

The investigation dashboard is a preset group of charts and a table that help you understand what is happening in your system at any given time, and upon which you can build your own customized dashboards.

There are two default FAM views, each with different charts and tables. Select the view from the dashboard menu . The default views cannot be modified.

Note: The Server IP and Client IP are always the same in the dashboard, except for the case of connecting through remote desktop on Windows. Client IP is only supported when connecting through a remote desktop session.

Note: The FAM queries the server for the server IP addresses and takes the first one it finds. There is no way to select "the appropriate" IP address from a host name when the host has multiple IP addresses. Specify explicitly the IP address you want to see in the reports.

The default dashboards contain data for the last hour presented in one or more of:

- Trimetric charts (3-axis data graphs). The default view is a color map. Additional views are bar graph, bubble graph, line graph, pie graph, step graph, and area graph.
- Results table: provides the search results and investigation features of the original quick search. The Results Table is always at the bottom of the dashboard. It can be added to any dashboard. Tabs are:
  - Activity: Summary and Details tabs showing monitored data, based on the file server policy rules. Each row in the Summary tab gives the number of instances of recorded access activities per server and OS user. The Details tab adds the Server Hostname, Server, Client Hostname, Client IP, OS user, File Full Name, Command, Date and Time. Each row in the Details tab gives full details on one activity. Data in the Activity tab is consistent with the date and time of the collector.
  - Outliers: see [Interpreting file activity outliers in the investigation dashboard](#)
  - Errors: Summary and Details tabs. Each row in the Summary tab gives the number of instances of reported errors per server and client IP, and the date. The Detailed Summary adds the error details, and the time. Each row in the Details tab gives full details on one error.
  - Violations: Summary and Details tabs. Each row in the Summary tab gives the number of instances of recorded violations per server, source program and OS user combination. The Detailed Summary adds the Client IP, severity, violation and violation details, date, and time. Each row in the Details tab gives full

- details on one violation. Data in the Violations tab is consistent with the data and time of the file server.
- Entitlement: Summary and Details tabs. For file servers, this tab presents sensitive data based on the current FAM decision plans. Each row in the Summary tab gives the number of instances of recorded access activities per server and owner. The Details tab adds the Server Hostname, full path, Type, , Size, Classification Entities (the decision plan that caused this file to be identified as sensitive), Owner, Client Hostname, Client IP, OS user, File Full Name, users and groups with write, read, execute, and delete permissions, last modification, Version (Sharepoint only), creation time, Date, and Time. Each row in the Details tab gives full details on one activity. You can use the data in this table to create policy rules and groups for file servers, see [Creating a FAM policy rule from the Investigative Dashboard Entitlements tab](#).

Additional views that you can add or open are:

- Topology view  : see [Using the topology view](#)
- Animated bubble chart: an animated visualization of data changes over the last 48 hours. The chart depicts the behavior of objects over a period of 24 hours. Each object is depicted as a circle, and its area and position (x and y axis) represent three user-selected variables. The animation represents the object's behavior over the 24 hours. Access from the Add Chart drop-down.
- Activity chart: a line chart that displays the volume of activity and outliers, located above the Results table. Access from the Add Chart drop-down.

Controls and options on this page:

- A categorized facet list of Where, Who, What, Exception, and When, from the search results appears on the left side of every dashboard and cannot be removed. Filter the entire dashboard by the specific facets, by expanding the list and clicking on individual facets.
- The Active Filters row at the top of the window shows the current filters. Delete filters by clicking the .
- Search field: free text search that filters the results in all fields simultaneously, irrespective of facet and no case-sensitivity. Exceptions:
  - anomaly score does not support < or >
  - Searching in a specific field is case-sensitive. For example, when searching "Source Program=nnnnn" nnnn must match a value in the facets.
- Distributed search: see [Local and distributed search](#)
- Time period for which data is presented: modify by clicking the drop-down in the upper right corner. Options are last 1 hour, last 3 hours, last 1 day, last 3 days, any time period you specify. Default is one hour.
- Filters drop-down: see [Filtering data and saving filters in the investigation dashboard](#)
-  : see [Creating, saving, and exporting investigation dashboards](#)

## Related concepts

- [Interpreting file activity outliers in the investigation dashboard](#)

## Related tasks

- [Using the topology view](#)

# Filtering data and saving filters in the investigation dashboard

## About this task

You can filter data in the entire investigation dashboard, and in an individual chart. You can drill down from the Results Table into related information.

You can save filters for your future use. When you save a filter set, you choose if you want to share it, and choose the roles that you share it with.

## Procedure

- Use the rules and syntax to filter data. All of these are relevant for both the Details and Summary tab, except where noted.
  - To match an exact phrase, use double quotation marks around the search terms. For example, "**Profiling Alert List**" returns entries for Connection Profiling Alert List but not for Profiling List Alert.
  - To match all specified search terms, separate the terms with a space. For example, **Hadoop getlisting** returns any entries that contain both Hadoop and getlisting in any location or sequence.
  - To match any specified search terms, separate the terms with OR or a vertical bar (|). For example, **Hadoop OR getlisting** returns any entries that contain either Hadoop or getlisting in any location.
  - To exclude a specified search term, use NOT or a period (.). For example, **NOT Hadoop** does not return any entries that contain Hadoop in any location.
  - Wildcards are supported by using asterisks (\*) at the beginning or ending of a string. For example, **10.10.70.\*** returns any entries with the string 10.10.70. followed by any additional characters.
  - Search rules can be used in combination. For example, **2016-5-08 (19.\*|20.\*)** returns results in the time range of May 8 between the hours of 19:00:00 – 20:59:59.
  - To match an exact phrase in a specific column, enter "**field name=value**", for example "**DB USER=user123**". This search syntax is the only case-sensitive syntax. In the Details tab, you can also use this search for columns with numeric values with search values of < >. For example, "**Total Instances>1**". This is particularly useful when there results on multiple pages and you cannot see the full list of possible values.

Adding filters changes each view based on the *RefFilter* specified for the view. Current filters appear in the menu bar. Each one can be cleared by clicking its X.

- Refine search results with any of the following methods:
  - Select specific filters based on the facets list:

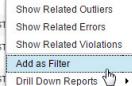
- Click the x or y-axis headers of a chart.
- Click an individual search result in the Results Table:

| Source Program   | DB User  | OS User | Client Hostname |
|------------------|----------|---------|-----------------|
| DB2JCC_APPLICATI | DB2INST1 |         | PIPPIN          |
| DB2JCC_APPLICATI | DB2INST1 |         | PIPPIN          |
| DB2JCC_APPLICATI | DB2INST1 |         | PIPPIN          |

Note: You can select one or more rows and right-click one of the server/DB user/Client IP cells to add them to an existing group, or to create a new group.

3. Drill down by individual results by right-clicking on specific search results and exploring related outliers, errors, or violations, or viewing one of several available drill-down reports.

| Source Program   | DB User  | OS User | Client H |
|------------------|----------|---------|----------|
| DB2JCC_APPLICATI | DB2INST1 |         | PIPPIN   |



4. To save a filter set, click Filters > Save. Provide a name for the filter and mark it as Private or click Share with to share the filter with specific roles. To save as your default filter set (dashboard always opens with these filters), select Set as default filter. When you are finished, click OK to save the filter.

## Filtering an individual chart

You can filter an individual chart. The  icon becomes red when specific filters are set for a chart that are different than the general dashboard filters. Hover over the icon to see which filters are used in that chart.

### About this task

A chart can have filters set as inactive, which means the chart data is not filtered by that field. This enables Guardium® to display other items, in addition to the ones related to the case, that may be similar or in some way provide additional insight into the investigation.

Example: While investigating activity on a server, you want to compare one of the charts with data from other servers. This is possible by deactivating the Server filter for just that one chart. To do this, you would click the  icon and select the Inactive radio button for the Server row.

### Procedure

1. Click the  icon.  
The Chart Filter Settings opens.
2. Click or clear the radio buttons as relevant, and click Apply.

## Creating, saving, and exporting investigation dashboards

### About this task

There are many ways of filtering the data in the dashboard. Filter sets can be private or shared. For example, a person who is knowledgeable about the environment can set up relevant filters. This person can create the filters for a specific investigator and then share the filter with that role. You cannot change and save the predefined system dashboards under their original names.

Important: All investigation dashboards are public. When a dashboard is saved, all users who have access to dashboards also have access to the saved dashboard through the dashboard menu. In addition, if you save a dashboard as the default dashboard, all users see that default.

You can use the same dashboards with different filter sets, depending on what data you want to see.

Example: Your dashboard includes an activity chart that shows the activities of database users with a breakdown by client IP. You want to view the same data filtered by different databases, such as HR versus Financial. You might want to add different command types for each database as well.

- Filter 1: by database HR, by verb SELECT
- Filter 2: by database FINANCIAL, by verb UPDATE

You can open the same dashboard and toggle through the different filter sets associated with that chart by using the and icons above the Active filters list. Any investigation dashboards, including threat diagnostics, can be encrypted and exported for sharing. Only the dashboard definitions are exported, not the filters.

If you have a dashboard that is configured with a good set of charts for investigating particular incident types, you can share this knowledge with other Guardium users without including actual attack data or revealing the filters.

## Procedure

1. To save the current display, click the icon.
2. To save a dashboard with a different name for modification and subsequent use, click the icon, and save it with a descriptive name and optionally a category.  
You can also define a category when you save the dashboard. The name and category can include spaces. To retrieve the dashboard later, click the icon to open the dashboard menu.
3. To export investigation dashboards, go to [Manage > Data Management > Definitions Export](#). From the Type menu, select Investigation Dashboard and select the dashboard definitions to export. Then, click Export.

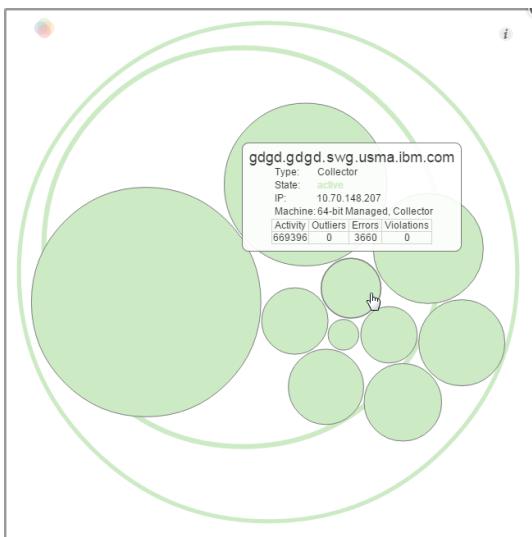
## Using the topology view

The topology view is visualization of the Guardium® appliances in the search results.

### About this task

You can view details about each server, select filter criteria, narrow search results to specific segments of the overall Guardium environment. Solid circles represent collectors and aggregators. Outlined circles represent Central Managers. The color of the circle indicates the status of the server. The outline color of the Central Manager indicates its status. The size of the circle indicates the relative volume of the collected data.

The topology view is not supported on stand-alone machines.



## Procedure

1. To open the topology view, click the Search server status view icon in the toolbar of the investigation dashboard.
2. Hover the mouse over an object to display detailed information about that object.



3. Select an object to narrow the search results to only that object and its children if any exist. Use Ctrl + click to select or deselect multiple objects in the topology view.
4. Close the topology view by clicking the close icon or clicking outside the topology browser. The search results update automatically to reflect the available data based on the scope selected in the topology view.

# Local and distributed search

## About this task

The Investigative Dashboards can run in either local or distributed modes. In local mode, searches are limited to the data available under the local machine (the machine from which the search is run). For example, a local search that is run from an individual collector returns results from data sources under that collector but not from any data sources under other collectors in the environment. In distributed mode, searches return data from across the entire Guardium® environment and results are not limited by the specific machine on which the search is run. A topology tool is provided to conveniently narrow search results to specific segments of the overall Guardium environment.

Investigative Dashboards default to local search mode.

## Procedure

1. To toggle between local or distributed search, click the Enable / Disable search all appliances icon  in the search window toolbar.  
Search results automatically update to reflect the available data based on the selection of local or distributed search.
2. See [Using the topology view](#) for information about filtering global search results by a specific segment of the Guardium environment.

# Monitoring and automatic recovery for the Investigation Dashboard

Use Monitoring and automatic recovery to identify and recover issues in the investigation dashboard.

Monitoring and automatic recovery is a process that monitors the engine behind the investigation dashboard. When Monitoring and automatic recovery detects issues, it displays them in the deployment health, lists their status, and runs the necessary steps to recover issues that can be recovered automatically.

If Monitoring and automatic recovery cannot recover an issue automatically, it displays the issue in the report under a different status. You can then troubleshoot those issues further.

Monitoring and automatic recovery is enabled by default and runs every 20 minutes on the central manager. It displays the issues that it finds in deployment health and in predefined admin reports. In those reports, the issues are further broken down per status (Open, In recovery, and All issues).

- [Viewing the Investigation Dashboard's status in deployment health views](#)  
View and monitor the Investigation Dashboard's status from deployment health views.
- [Viewing Investigation Dashboard issues in reports](#)  
You can see issues for the Investigation dashboard in various reports.
- [Viewing the Investigation Dashboard Issues alert for the Investigation dashboard](#)  
Receive alerts for new Investigation Dashboard issues that cannot be resolved automatically.
- [Addressing Investigation Dashboard issues](#)  
Learn about the different Investigation Dashboard issues and what you can do about them.
- [Running manual intervention for Investigation Dashboard issues](#)  
Understand when you need to run manual intervention for Investigation Dashboard issues, and which intervention steps to take.

## Viewing the Investigation Dashboard's status in deployment health views

View and monitor the Investigation Dashboard's status from deployment health views.

Status for Investigation Dashboard issues can be viewed from the deployment health table, deployment health topology, and deployment health dashboard. Issues are designated the status of No issues (green), Medium (orange), and Status unavailable (blue).

For example, the Investigation Dashboard column in the health deployment table displays a green, orange, or blue circle for each issue to indicate its status. The Details column of the same table provides more details as needed.

- A green circle without details in the Details column means that there are no issues on this unit at this moment.
- A green circle together with details in the Details column means that an issue is in recovery.
- An orange circle indicates that an open issue is detected and cannot be repaired automatically. A manual fix is required.
- A blue circle means that a unit is down or something is unavailable.

For more information, see [Deployment health topology and table views](#).

## Viewing Investigation Dashboard issues in reports

You can see issues for the Investigation dashboard in various reports.

Investigation dashboard issues can be viewed in the following reports:

- Investigation dashboard open issues. This report displays issues that the Monitoring and automatic recovery was not able to fix and require manual intervention to be resolved. Follow the manual fix recommendations or contact IBM Support.
- Investigation dashboard issues in recovery. This report displays issues that Monitoring and automatic recovery is trying to fix.
- Investigation dashboard issues. This report includes all issues, including issues that are open, in progress, and fixed.

For more information, see [Predefined admin reports](#)

# Viewing the Investigation Dashboard Issues alert for the Investigation dashboard

Receive alerts for new Investigation Dashboard issues that cannot be resolved automatically.

Alerts for the Investigation dashboard are designed to notify you of every new issue that cannot be resolved automatically.

For more information, see [Predefined alerts](#).

## Addressing Investigation Dashboard issues

Learn about the different Investigation Dashboard issues and what you can do about them.

Various Investigation Dashboard issues can appear in several reports, alerts, and deployment health views. To see what the various issues mean and what actions you can take regarding each one, see the following table.

| Issue                                                     | Description                                                                                                                                                                                                                                       |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The core is down.                                         | The Investigation dashboard isn't able to show data indexed in this core type from this collector. (For example, if ERROR_5 core is down, the Errors tab shows no data from this collector).                                                      |
| The node is missing.                                      | The Investigation dashboard isn't able to show data indexed in this missing node type from this collector. (For example, if ERROR_5 node is missing, the Errors tab shows no data from this collector).                                           |
| The core has a redundant replica and the replica is down. | The redundant replica is not needed. Since it is down, it is better to remove it. The user is not impacted.                                                                                                                                       |
| The core has a redundant replica. All replicas are down.  | The Investigation dashboard is not able to show data that is indexed in this core type where all its replicas are down from this collector. (For example, if ERROR_5 core's replicas are down, the Errors tab shows no data from this collector). |
| The collection configuration is incorrect.                | The Investigation dashboard isn't able to show data indexed in this collection type from all appliances. (For example, if the ERROR_5 configuration is wrong, the Errors tab shows no data from all appliances).                                  |
| The cores are down for the specified collection.          | The Investigation dashboard isn't able to show data indexed in this core type from this collector. (For example, if ERROR_5 cores are down, the Errors tab shows no data from this collector).                                                    |
| The unit is not listed in the cluster.                    | The Investigation dashboard isn't able to show data indexed on this collector.                                                                                                                                                                    |
| Incorrect hostname                                        | The Investigation dashboard isn't able to show data indexed in this core type from this collector. (For example, if ERROR_5 core is down, the Errors tab shows no data from this collector).                                                      |
| Data is not being indexed.                                | The Investigation dashboard isn't able to show data indexed in this data mart type from this collector. (For example, if Lucene Exception data mart is not running, the Errors tab shows no data from this collector).                            |
| Data indexing failed                                      | The Investigation dashboard isn't able to show data indexed in this data mart type from this collector. (For example, if Lucene Exception data mart fails, the Errors tab shows no data from this collector).                                     |

## Running manual intervention for Investigation Dashboard issues

Understand when you need to run manual intervention for Investigation Dashboard issues, and which intervention steps to take.

Monitoring and automatic recovery attempts to fix the issues it finds by running several recovery actions. If these attempts fail, you need to intervene manually.

To figure out when to intervene and how, first go to the Investigation dashboard open issues report. In the report, check the most recent automatic repair action that displays next to each open issue. Then, refer to the manual intervention recommendation for that repair action in the following table. In cases where your intervention still does not resolve the issue, contact IBM Guardium support.

| Last automated repair action                                                                                 | Recommendation                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Quick Search is disabled on the managed unit. The hardware requirements are not met. Awaiting manual action. | For more information, see <a href="#">minimum hardware requirements</a> .                                                                                                                                                                                                                                                                                    |
| Quick Search is disabled on the unit. Awaiting manual action.                                                | Enable the Investigation Dashboard with the GuardAPI command.<br><br>For more information, see <a href="#">this topic</a> .                                                                                                                                                                                                                                  |
| Quick Search is down. Attempt to restart Quick Search.                                                       | Restart Solr manually. Run the restart_solr grdapi.<br><br>For more information, see the <a href="#">restart_solr topic</a> .                                                                                                                                                                                                                                |
| Verify that the managed unit is set up correctly on the central manager.                                     | Unregister and register the unit. For more information, see the topics about <a href="#">registering</a> and <a href="#">unregistering</a> units.                                                                                                                                                                                                            |
| Attempt to ping Quick search ports (8983, 9983).                                                             | Test connectivity in the cluster by running the GuardAPI test_solr_connectivity on the central manager.<br><br>For more information, see the <a href="#">test_solr_connectivity topic</a><br><br>Verify connectivity for ports 8983 and 9983 between the central manager and managed units.<br><br>Check on both internal (Guardium) and external firewalls. |

| Last automated repair action                                                                                                                  | Recommendation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Verify that the core hostname is set up correctly.                                                                                            | <p>Verify that the unit hostname is set up correctly. There are multiple ways to do so.</p> <ul style="list-style-type: none"> <li>CLI command of store system hostname. For more information, see this <a href="#">topic</a>.</li> <li>Verify that the correct hostname appears on the central manager. On the central manager, go to <b>Manage &gt; Central Management &gt; Central Management</b> and check the hostname for your unit. If the hostname is incorrect, run <b>Refresh Unit Info</b>.</li> </ul> <p>If neither of these methods resolve the issue, contact IBM support to run a clean Solr upgrade.</p> |
| Validate that the unit type is set up correctly.                                                                                              | If the issue remains unresolved after a few hours, contact IBM Guardium support.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| The core was replicated and one of the cores can't be reached. Attempt to remove the unreachable core.                                        | If the issue remains unresolved after a few hours, contact IBM Guardium support to re-create the core.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| The core is down and the collection can't be reached. Attempt to create a new core instead of the old one without copying the data.           | If the issue remains unresolved after a few hours, contact IBM Guardium support to re-create the core.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| The core is down and the collection can't be reached. Attempt to create a new core instead of the old one with the data from the old core.    | If the issue remains unresolved after a few hours, contact IBM Guardium support to re-create the core.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| The core was replicated and both cores can't be reached. Attempt to create a new core instead of the old one without copying the data.        | If the issue remains unresolved after a few hours, contact IBM Guardium support to re-create the core.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| The core was replicated and both cores can't be reached. Attempt to create a new core instead of the old one with the data from the old core. | If the issue remains unresolved after a few hours, contact IBM Guardium support to re-create the core.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| The cores are down for the specified collection. Attempt to create a new core instead of the old one without copying the data.                | If the issue remains unresolved after a few hours, contact IBM Guardium support to re-create the core.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| The cores are down for the specified collection. Attempt to create a new core instead of the old one with the data from the old core.         | If the issue remains unresolved after a few hours, contact IBM Guardium support to re-create the core.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| The unit is not listed in the collection's cluster. Attempt to create a new core instead of the old one without copying the data.             | If the issue remains unresolved after a few hours, contact IBM Guardium support to re-create the core.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| The unit is not listed in the collection's cluster. Attempt to create a new core instead of the old one with the data from the old core.      | If the issue remains unresolved after a few hours, contact IBM Guardium support to re-create the core.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Attempt to restart quick search.                                                                                                              | Unregister and register the unit. For more information, see the topics about <a href="#">registering</a> and <a href="#">unregistering</a> units.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| The creation of the collection failed because the collection configuration is incorrect. Awaiting manual fix.                                 | If the issue remains unresolved after a few hours, contact IBM Guardium support.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| The configuration manager is running on the managed unit. Attempt to stop the configuration manager process on the unit.                      | If the issue remains unresolved after a few hours, contact IBM Guardium support.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| The unit is listed in the incorrect configuration manager.                                                                                    | Restart Solr manually. Run the <code>restart_solr gradapi</code> . For more information, see the <a href="#">restart_solr topic</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| The indexing process is not scheduled. Attempt to resume or reschedule the indexing job.                                                      | Restart the UI manually. For more information, see the restart GUI section in <a href="#">Configuration and control CLI commands</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Verify that the indexing process ran in the last hour.                                                                                        | Restart the UI manually. For more information, see the restart GUI section in <a href="#">Configuration and control CLI commands</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| The indexing process failed.<br>Awaiting manual fix.                                                                                          | If the issue remains unresolved after a few hours, contact IBM Guardium support.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Threat Detection Analytics

Guardium includes specialized threat detection analytics that scan and analyze audited data to detect symptoms that may indicate different types of database attacks.

Threat detection analytics scans and analyzes audited data to detect symptoms that may indicate SQL injection or Stored Procedure database attacks. Guardium does not rely on a comparison against an ever-changing dictionary of attack signatures. Instead, Guardium analyzes audit data activity, exceptions, and outlier data ([Outliers detection](#)) over extended periods of time looking for patterns that indicate an attack. By tracking the suspicious events over time and correlating them, Guardium creates a comprehensive picture of potential risks. This approach is more flexible and comprehensive, and does not require continual signature updates.

Threat detection analytics is supported on MSSQL, MySQL, Oracle, and Db2.

- [Characteristics of an SQL injection attack](#)

SQL injection attacks attempt to exploit web application vulnerabilities by concatenating user input with SQL queries. If successful, these attacks can execute malicious SQL commands by using the legitimate web application connection. SQL injection attacks can be difficult to identify because the individual steps of an attack, analyzed independently of the other steps, might be considered legitimate.

- [Characteristics of a stored procedure attack](#)

A malicious stored procedure is a block of code that is designed to evade detection, and to perform complex attacks over a period of time. The exact attack can be repeated, or it can change its characteristics over time.

- [Enabling and disabling threat detection analytics](#)

Understand the prerequisites and procedures for enabling threat detection analytics.

- [Viewing case reports](#)

View case reports in threat analytics.

- [Activating the audit process workflow for threat analytics](#)

This procedure describes how to schedule the audit processes and distribute the threat analytics results for Suspected Malicious Stored Procedures and Suspected SQL Injection cases.

- [Working with threat diagnostic dashboards](#)

A dashboard that is invoked from a specific threat case in either the Suspected malicious STP Cases (stored procedures) or Suspicion SQL Injection Attacks report is

called a threat diagnostic dashboard.

## Characteristics of an SQL injection attack

SQL injection attacks attempt to exploit web application vulnerabilities by concatenating user input with SQL queries. If successful, these attacks can execute malicious SQL commands by using the legitimate web application connection. SQL injection attacks can be difficult to identify because the individual steps of an attack, analyzed independently of the other steps, might be considered legitimate.

Using threat detection analytics, Guardium identifies potential SQL injection attacks by capturing the individual steps and analyzing them as part of a single complex attack.

Typical symptoms of SQL injection attacks that Guardium identifies include:

- An attacker that is trying to identify the structure of a dynamic SQL query, for example the number of columns queried.
- An unusually large quantity of new queries, specifically queries that are uniquely or unusually structured.
- Access to tables that contain information about the database structure.

## Characteristics of a stored procedure attack

A malicious stored procedure is a block of code that is designed to evade detection, and to perform complex attacks over a period of time. The exact attack can be repeated, or it can change its characteristics over time.

The stored procedure can be dormant for an extended period of time, making it harder to identify as suspicious. Even if unusual activity was noticed in a previous audit, by the time the next audit occurs the previous activity is forgotten. A malicious stored procedure can be used to disguise a drop of an important table, or to extract the contents of a table.

Examples of suspicious activity are:

- Creating a stored procedure with a DROP statement with sensitive objects.
- A DROP verb.
- SQL exceptions that are caused by missing objects.
- A procedure that is modified after it was dormant for an extended period of time.

Guardium tracks the activity around individual stored procedures, and together with Outlier mining data correlates the various symptoms and users. Guardium can detect these typical symptoms of this malicious stored procedure use case (presented in the order they typically occur):

1. A database administrator creates a malicious Procedure A, which deletes data from the customer table.
2. A month later the database administrator changes a commonly used Procedure B to call Procedure A.
3. A different user calls the modified Procedure B, such that the customer table data is deleted by that innocent user.

## Enabling and disabling threat detection analytics

Understand the prerequisites and procedures for enabling threat detection analytics.

Threat detection analytics is enabled, by default, on Guardium versions 10.1.4 and higher.

To enable threat detection analytics:

- Ensure that you meet the minimum required memory and storage requirements for search (4 CPU and 24 GB RAM).
- Verify that your system has logged application data. Specifically, SQLI requires application data because the injection initiates from the application. If the system "trusts" the application and does not monitor it in Guardium, the injection cannot be identified.
- Outlier detection is not required for SQL injection threat detection but it is required to fully support malicious stored procedure detection. For more information, see [Enabling and disabling outliers detection](#).
- Enable threat detection scanning on each collector or on multiple managed units from the central manager by using the Guardium API command: `grdapic enable_advanced_threat_scanning`. See [Threat detection analytics APIs](#) for more information about parameters available for the `enable_advanced_threat_scanning` command.
- Set up the audit process to send case reports to the relevant investigators. This is optional but recommended. See [Activating the audit process workflow for threat analytics](#) for more information.

Important: Threat detection relies on analysis and correlation of logged data. Thus, any rules that filter out traffic before logging are not considered for threat detection. Examine your use of IGNORE S-TAP SESSION rules carefully to determine the risk of not logging these sessions versus optimizing the capacity of the collector.

To disable threat detection analytics, use the Guard API command: `disable_advanced_threat_scanning`, either on individual collectors, or from the central manager.

## Prerequisites for malicious stored procedures analytics

- The analytics algorithm depends in part on sensitive objects groups. By default, the algorithm uses members in the system-defined sensitive objects group (group ID 5). If you already specified other sensitive object groups for outlier detection, threat detection uses the same groups. Even if outlier detection is not enabled, you can set your own sensitive object groups by using the same GuardAPI command:

```
set_outliers_detection_parameter parameter_name="sensitiveObjectGroupIds" parameter_value=<group ID>,<group ID>,...
```

- Policy rules must be installed to collect the necessary traffic for malicious stored procedure analysis.

Recommendation: Create the following rules in your policy in the suggested order. It is important to check the Continue to next rule checkbox for all these rules.

1. Access rule: Log Full Details where Command group filter is PROCEDURE DDL.

2. Access rule: Log Full Details where the Command group filter is EXECUTE Commands. If your database is Oracle, include the command BEGIN in the rule.

3. Exception rule: Log Only where the error type filter is SQL\_ERROR.

## Related reference

---

- [Threat analytics APIs](#)

## Viewing case reports

---

View case reports in threat analytics.

Guardium analyzes the symptoms over time, correlates them, and assigns a score per identified possible attack. If the score indicates a likely attack, the set of events becomes a case whose ID is unique per collector. Cases are externalized in case reports, one per each suspected attack. Access case reports in one of the following ways:

- Set up an audit process to receive notifications in your To-Do list on the Central Manager, and open the report directly on the relevant associated collector. The To-Do list is updated once an hour.
- Access the reports in the UI by going to [Investigate](#) > [Exceptions](#).

In the case reports window, a case report presents, by default, up to 3 incidents (one per line). Each case includes a risk score from 1 to 3, with 3 being the most severe. In this window, you can:

- Hover on the case ID to view a summary of the attack (only stored procedure cases).
- Hover on the case ID and click [Link to Symptoms](#) to access the detailed symptoms report.
- Click the ID to open the case-specific threat diagnostic dashboard. See [Working with threat diagnostic dashboards](#).

Restriction: Case reports have the following restrictions:

- Data Level Security is not available.
- These reports cannot be cloned.
- You can create a distributed report for these case reports. However, the central manager does not provide direct links from the case report to the threat diagnostic dashboard. Additional hover help and links to symptoms are not available.

## Activating the audit process workflow for threat analytics

---

This procedure describes how to schedule the audit processes and distribute the threat analytics results for Suspected Malicious Stored Procedures and Suspected SQL Injection cases.

## About this task

---

Two preconfigured audit processes control the distribution of threat analytics reports to the appropriate reviewers:

- Suspected malicious STP Cases
- Suspected SQL Injection Cases

Each process pulls out the suspected cases on one attack type. You can customize these processes, or copy and create your own.

## Procedure

---

1. Go to [Comply](#) > [Tools and Views](#) > [Audit Process Builder](#). Optionally filter the available audit processes by clicking the [Inactive only](#) radio button or typing [Suspected](#) in the Filter box.  
The default task for this process is the corresponding report (Suspected malicious STP Cases or Suspected SQL Injection Cases). Do not modify the runtime parameters of these reports. However, you can add more tasks to this same audit process. For example, you can add both the threat reports into a single audit process.  
If you are defining these audit processes from a central manager, define a task for each collector for which you want to see threat data and use the [Remote Data Source](#) option.
2. Click [Send results](#) to define the audit process receivers who receive reports on suspected malicious stored procedures.
3. Select the default receiver (user) and then click the icon to define the appropriate receiver or receivers for your organization. When you are finished, click [OK](#).
4. Click [Schedule audit process](#) and review the schedule for the audit process.  
The recommendation is to run the process every day, every hour at 12:30 AM or later (after both outliers and threat detection usually run). Note that the checkbox [Auto run dependent jobs](#) has no effect for this task.

Important: Make sure that the [Activate schedule](#) checkbox is checked.

5. Click [Next](#) and then click [Save](#) to finish working with the audit process.

## Working with threat diagnostic dashboards

---

A dashboard that is invoked from a specific threat case in either the Suspected malicious STP Cases (stored procedures) or Suspicion SQL Injection Attacks report is called a threat diagnostic dashboard.

A threat diagnostic dashboard performs much like other investigation dashboards, except that the dashboard for that case is populated with the data from the suspicious events (db user, server, objects, etc.) and uses different charts to provide different views of the event and surrounding events that may be helpful in investigating the

possible attack. The relevant search and outlier data is also available on the same dashboard page as the charts.

In many cases, you will not need to change any of the preexisting filters for the predefined threat diagnostic dashboards. However, if you want to do some of your own comparative analysis, you can modify the preexisting filters.

See [Investigation Dashboard](#) for more information on working with dashboard and chart filters.

**Tip:** The threat diagnostic dashboard can only be opened by clicking on the case number in the relevant threat report. You cannot save changes to this dashboard or any other predefined dashboard. If you make changes and want to keep the dashboard for further investigation, you must copy it and save it under a new name. You must also save the filters by clicking the Filters menu and selecting Save.

Reference data is a set of predefined, chart-specific filters, for Threat Detection Analytics only, that show data similar to the case you're investigating but not included in the general dashboard filter. Reference data cannot be changed by users. Hover over the filter icon in each chart to see the Reference Data.

In a typical suspected malicious stored procedure attack, the threat diagnostic dashboard is filtered for this attack and includes the following general dashboard filters:

- Server: 8.34.223.145
- DB user: USER1
- Database: 8.4.134.213:31.5.12
- DB type: MYSQL
- Object: stp1\_name

The chart for DB user can include reference data for similar DB users, such as USER2, USER3 and USER4. This enables you to compare the activities of the suspected user with similar users, even though those additional users are not included on the general dashboard filters.

Not all fields include associated reference data. Any field for which there is no predefined reference filter is filtered as on the dashboard.

In some charts, filters can be inactivated so that you can compare data regardless of the filters chosen for the entire dashboard. This gives a wider picture of the activity.

Click the filter icon to open the Chart Filter Settings, and make modifications.

- [Investigating SQL injection threats](#)
- [Investigating stored procedure threats](#)

## Investigating SQL injection threats

### About this task

This procedure describes investigating a suspected SQL injection attack, using the threat diagnostic dashboard.

### Procedure

1. From the To Do list, or from [Investigate > Exceptions](#), open the Suspected SQL injection Cases dashboard. Each line is a case, with a Confidence (%) rating of certainty of an attack, and a risk level of the attack.
2. Click View to evaluate for false positives. Hover over the selected case id and click Symptoms to open the SQL Injection Case Symptoms page. Every suspicious action is described, and the SQL string displayed. You can see the exact modifications the user made to strings. By progressing from string to string, you can observe how the attacker methodically gained more data using errors returned from previous queries.
3. Click the id number to open the default diagnostic dashboard for SQL injection attacks, which is filtered by the incident's date and suspected web-application connection details. This helps narrow the investigation to database traffic that occurred during the attack. You can change or drop the filter to broaden the scope of investigation. Use the bottom grid to get more detailed information on the chart's data. Note that if you move to a standard dashboard, all filters specific for the suspected SQL injection attack are canceled.
4. Use these guidelines while investigating the charts:
  - Change the timescale to look for peaks at time of the attack
  - Look for violation of any security policy, and see if any violations correlate to other activity at the time of the attack
5. Drill-down by changing filters, timeframe, etc. to see if there are differences across the system.
6. Evaluate the charts in the dashboard:

#### Activities count per time and object

This chart contains the most used database objects in the time of the attack. By expanding the time frame of the dashboard you can compare the difference in activity before and after the attack. Click a cell if you want to filter for a particular object. The color indicates different object names.

#### Error count per time and error

This chart indicates how many SQL errors were generated by the web application. A high rate of SQL errors can indicate that some sort of SQL injection attack is taking place. The color indicates different error types.

#### Outlier count per time and outlier reason

An SQL injection attack involves a large number of new queries with a different structure than usual queries. Those queries generate outliers. Use this chart to see the volume and score of outliers generated by the offended web application.

#### Violations count per time and violation

During an SQL Injection attack the attacker is likely to violate security policies that log access to unauthorized objects. Compare the volume and types of violations to understand the risk of the attack.

#### Suspicious error types

Use this chart to explore specific SQL errors that are used in SQL injection attacks in order to exploit the vulnerability. Click a cell to filter the search and look at the SQL statement that generated this error. You may notice an injected SQL code.

#### Suspicious object names

Use this chart to view the suspicious objects that are used during SQL injection attacks. Expand the time frame of the search to see if those objects were used before the attack started. Compare the volume of the usage of those objects.

## Investigating stored procedure threats

## About this task

---

Investigate a suspected stored procedure attack by using the threat diagnostic dashboard.

## Procedure

---

1. From the To Do list, or from [Investigate > Exceptions](#), open the Suspected malicious STP Cases dashboard. Each line is a case. Each case shows a Confidence rating of certainty of an attack and a risk level of the attack.
2. Click View to evaluate for false positives.
3. Hover over the selected case ID to view the case details.
4. Click symptoms to open the Malicious STP Case Symptoms page.
5. Click the ID number to open the default diagnostic dashboard for SQL injection attacks, which filters according to the incident's date and suspected web-application connection details. This filtering helps to narrow the investigation to database traffic that occurred during the attack. You can change or drop the filter to broaden the scope of investigation. Use the grid on the page to get more detailed information on the chart's data.
6. Use these guidelines while you investigate the charts:
  - Change the timescale to look for peaks at the time of the attack.
  - Look for violations of any security policy, and see whether any violations correlate to other activity at the time of the attack.
7. Drill-down by changing filters, time frame, and more to see whether differences exist across the system.
8. Evaluate the charts in the dashboard:
  - Compare errors on different servers  
Use this chart to understand whether this server and DB user have exceptionally more errors than other servers and DB users.
  - Compare errors from different database users with similar behavior  
Use this chart to compare the error types and their volume on this DB user compared to similar DB users. The similar DB users are all users that created stored procedures.
  - Similar activities on stored procedures by this database user  
Use this chart to see stored procedures that the user created or modified at the specific period. The chart filters by verb. Use this chart also to drill down and see what the user did on the different stored procedures.
  - Compare violations from database users with similar behavior  
Compare the volume and type of violation (policy) on DB users that create stored procedures.
  - Compare outliers from database users with similar behavior  
Use this chart to compare the volume and type of outliers on this DB user with other DB users that create stored procedures.
  - Outliers by data on this database user  
Use this chart to see the volume and score of outliers on the specific DB user.

---

## Data Protection Dashboard

The Guardium® data protection dashboard provides a summary view of risk and compliance data intended for senior-level security officers.

The data protection dashboard contains several charts and graphs in addition to compliance and risk statistics designed for continuous display on a large monitor. To open the dashboard, navigate to [Investigate > Guardium Data Protection Dashboard](#).

View this dashboard on your central manager.

**CAUTION:**

The session does not expire and you are not automatically logged out while viewing the data protection dashboard. Use care when leaving the dashboard open for long periods of time.

Information:

- The dashboard automatically refreshes every 20 minutes.
- The default search settings are for distributed search with data collected from the previous one day.

---

## Charts and graphs

Several line charts allow you to quickly compare different types of data. For example, a chart can display the volume of activities, errors, and violations over time.

An Anomalous activities chart displays a summary of outliers in relation to overall activity. On this chart, an outliers summary dot represents an unexpected volume of outliers.

Information: The y-axis of these charts is a log axis and may distort the chart proportions, and the values or counts are not logged.

---

## Risk and compliance statistics

The Risk statistic shows the number of tests that failed with critical severity and the number of datasources where those failure occurred. Each datasource can have multiple failed tests.

Monitored datasources shows the number of datasources for which the system is logging activities. This statistic is calculated by looking at the available access domain data.

Compliance to-do list tasks shows the following summary of audit processes: the number of processes that were closed today, the number of processes that have been open for less than three days, and the number of processes that have been open for more than three days.

Information:

- Statistics are not affected by facet and text search filters, but statistics are affected by the search mode. To change the search mode, use the ▾ control to expand the top pane, then click the  icon to toggle between distributed and local search.
- The statistics components are recalculated once every hour.

## Building audit processes

Use the Audit Process Builder to streamline your compliance workflow process by consolidating, in one spot, database activity monitoring tasks such as: asset discovery; vulnerability assessment and hardening; database activity monitoring and audit reporting; report distribution; sign off by key stakeholders; and escalations.

Guardium audit processes provide the following capabilities:

- Audit processes support company privacy and governance requirements, such as PCI-DSS, SOX, Data Privacy, and HIPAA.
- The audit process can export audit results to external repositories for additional forensic analysis such as Syslog, CSV or CEF files, or external feed.
- Generate an Audit Process Log report that shows a detailed activity log for all tasks, including start and end times.
- The results of each audit process, including the review, sign-off trails, and comments, can be archived and later restored and reviewed through the Investigation Center (if enabled). For more information, see [Restoring and viewing audit results in the investigation center](#).

Elements of the compliance workflow automation process can include,

- A process definition
- A set of tasks
- A distribution plan that defines the following elements:
  - Receivers - Individual users, user groups, roles, email, or ticket.  
Note: To configure tickets, you need to set up external ticket service for alerts. For more information, see [Configuring an external ticketing system](#).
  - The review and signing responsibility for each receiver.
  - The distribution sequence by setting the Continuous flag.
- A schedule - The audit process can be run immediately, or you can run the process regularly on a defined schedule.

## Creating an audit process

To start building an audit process, go to Comply > Tools and Views > Audit Process Builder.

1. From the Audit Process Builder page, click the  icon to open the Create New Audit Process page.
2. Click Name and archive to enter a name for your audit process.
3. Click Show advanced options to manage the following optional information.
  - Archive - Store a copy of audit process output after the retention period has expired. If needed, you can restore archived results.
  - Allow results to be purged prior to review - Deletes the results of an ad hoc process before all workflow activities have finished, such as reviews and sign-offs. This feature allows you to delete results in a specified period (such as 1 day) even if the results have not been reviewed.
  - Keep for a minimum of x days or y runs - Determine how long to keep the archived files. You can select either the number of days or then number of runs to archive. When a new archive file is stored, Guardium deletes the oldest file.
  - CSV/CEF file name - Provide a label for CSV or CEF files that are generated by audit processes.
  - Zip CSV for email - When emailing the file, select whether to compress the file before it is sent.  
Note: Guardium cannot export CSV files larger than 10 GB. Guardium recommends that you select Zip CSV for mail.
  - Email subject - The subject line for all emails for all receivers for that audit process. The subject can include one (or more) of the following variables. The variable is replaced with the following information:
    - %%ProcessName - The audit process description.
    - %%ExecutionStart - The start date and time of the first task.
    - %%ExecutionEnd - The end date and time of the last task.
  - 12.1 and later Custom email template- Use an existing custom email template or create a new template. To create a new template:
    - Click the New icon to open the New Template window.
    - Provide a unique name for the template.
    - Create the message that you want to include in the email. The message can include basic HTML options as well as the following messages:
      - %%ExecutionEnd - Process execution end timestamp.
      - %%ExecutionStart - Process execution start timestamp.
      - %%ProcessName - The name of the audit process.
      - %%UserAction - Required user action, which can be review or sign.
    - Click OK to save your new template.

The email template that you saved is available from the Global profile Named Template Finder window. For more information, see [Global profile](#).

Note: You can also create a custom email template from Named Template on the Global Profile page. For more information, see [Creating or updating named messages](#).

4. Export results - Specify whether to export results when an audit process runs, based on how export results are configured on the Results Export (Files) page. For more information, see [Exporting \(files\) results](#).

Note: If you do not configure the export results, these settings are ignored (and audit process results are not exported).

Specify when to export the results,

- Select Disabled to export results based on the configuration that you set in Results Export (Files).
- Select At the end of the process to export the results after the audit process successfully completes.
- Select At the end of each task to export the result after each task within the audit process completes.

5. Roles - By default, an audit process is assigned to a user with *audit process* privileges. Select Roles to open the role window and select other roles that can access this audit process.

6. Click Next to open Add tasks. Click the  icon to begin adding a task. You must define at least one audit task before you can save the process. Each type of task requires different information. For more information about creating and configuring tasks, see [Audit process task types](#)

Attention: For most task types, you need to define other steps first (such as creating a security assessment or privacy set). Guardium suggests that you make sure that you create the required scenarios before you start building the audit process.

7. After you name the audit process and add one task, click Save to save your work. If needed, add more tasks.

8. Click Send results to add or change who receives the audit process results. From the Receiver table, click the New icon to begin adding a receiver. Each receiver type provides different options. For more information about receivers and receiver types, see [Audit process receivers](#).

9. Click Schedule audit process to configure a schedule for running the audit process. For more information, see [Scheduling](#).

Note: Scheduling applies only to the Guardium unit on which you are defining this audit process. To manage an audit process from a central manager, you can create a distribution profile. For more information, see [Working with configuration profiles](#).

10. To test the audit process, select Run audit process and then click Run once now.

Users with the audit-delete role can delete audit process results. If you have audit-delete privileges, Delete Results displays in the Run audit process ribbon. Audit activity is tracked in the User Activity Audit Trail report.

Note: Audit process results from remote sources are limited to 100,000 results. To change that limit, use the **store save\_result\_fetch\_size** CLI command.

9. Click Save to save your changes or Reset to clear all of the changes you made since the last time you saved your work.

To add comments for the audit process, click the audit process name and then Show advanced options, and in the Comments window, click the New icon.

## Stopping an audit process

---

You can stop audit processes that are currently running or that have not run yet. Stopping an audit process does not deliver partial results; the audit process stops and returns a stopped error message. However, if tasks are complete, the results are still sent.

To stop an audit process from the Audit Process Log (Comply > Tools and Views > Audit Process Log), run the [stop\\_audit\\_process](#) GuardAPI by taking one of the following steps,

- Click the Actions menu, and select **stop\_audit\_process**.
- Place your cursor on any line, right-click to open the pop-up menu. Select Invoke and then select **stop\_audit\_process**.

For any user, stopping an audit process displays only the line that belongs to that user (just the tasks, not all the details). An admin user can see all the details and can stop anyone's audit processes. A user can stop only their own audit processes.

To stop an audit process on a remote source, select **stop\_audit\_process** from a line (not the Action menu) and specify the Target Host , which can be a group of managed units or the IP address of a managed unit.

Note: You cannot stop running audit processes for Privacy Sets Audit Tasks or External Feed Audit Tasks. If the Privacy Set or External Feed tasks are running, they finish even if the process is stopped.

## Adding workflow events

---

Define a formal sequence of event types for certain tasks.

1. From the Audit Process Builder, create an audit task.
2. Depending on the task, Events and Additional Columns displays on the Edit task window.  
For example, the Events and Additional Columns is displayed on the Edit task window for the *Report* Task type and the *Admin Users Login* report.
3. Click Events and Additional Columns to display the Event & Sign-off window. The workflow that you created appears as a selection in Event and Sign-off.
4. Highlight this choice and click Apply to save your selection.
5. If you need to add additional information (such as company codes, or business unit labels) as part of the workflow report, add this information under Define Additional Columns then click Add. To select a predefined or created groups column, change the Type column to Group.
6. When you are done, click Close this window.
7. Click OK to save the task and then Save to save the entire audit process definition.

Notes:

- Under the Report choices are two procedural reports that are available to admin users (and users with the admin role), Outstanding Events and Event Status Transition. Add these two reports to two new audit tasks to show details of all workflow events and transitions. These reports are not filtered (observed data level security filtering is not applied).
- Additional Columns is unavailable for some tasks.
- When you clone a process, the task that is associated with the process is added to the cloned process. But, if you make changes to this task, the workflow that is associated with the original task is not cloned.
- You can delete an event status only if the status is not in the first status of any events, and if it is not used by any action. The validation provides a list of events or actions that prevent the status from being deleted.
- The owner or creator of a workflow event can always see all statuses of this event, regardless of what roles are assigned to these statuses.

For more information about the Workflow builder, see [Workflow Builder](#).

## Audit processing notes

---

- On a central manager, reports can reference data from remote datasources (managed units). Audit processes that use these reports are accessible from the central manager only, and cannot be seen from managed units.
- Use the [store max\\_audit\\_reporting](#) CLI command to configure the audit report threshold.  
When you define reports, make sure that the number of days (defined by the FROM-TO fields) does not exceed a certain threshold. The default threshold is one month. If this threshold is exceeded, a runtime error results when the audit task runs on the aggregator.

No warning message displays when you create a report with an invalid FROM-TO range. Instead, an error displays in the Task Parameters window in the Audit Process setup page.

- You can create an audit task with a FROM-TO range that is wider than the value of the [store max\\_audit\\_reporting](#) CLI command. Audit processes defined on the aggregator can be run on managed collectors (when this aggregator is a manager). Audit tasks that are run on collector unit do not have a max\_audit\_reporting limitation.
- You can use audit processing for the aggregator server to create ad hoc databases for each aggregator task and specify only the relevant days for that task. You can keep the ad hoc databases for the aggregation server in the system for up to 14 days (depending on the value of the [store aggregator drop ad\\_hoc\\_audit\\_db](#) CLI command). If needed, use these databases for post-run analysis by Guardium support services.
- All audit processes are stopped when a patch installation runs.
- **Audit process task types**  
When you create an audit process with the Audit Process Builder, you need to select the database activity monitoring tasks to include in your audit process. Create the monitoring activities that you want to include before you start building the audit process.
- **Audit process receivers**  
Use the audit process builder to send audit process output to many different people or groups (receivers). These process receivers can view and manage audit process output.
- **Exporting audit results**  
Reports that contain information that can be used by other applications, or reports that contain large amounts of data, can be exported to other file formats.

- [How to distribute workflow through Guardium groups](#)

Using the receiver group option, define a single Compliance Workflow audit process that will send different results to different Guardium users based on a pre-defined, custom mapping.

- [Audit Process To-Do List](#)

Use the Audit Process To-Do List to track tasks that are assigned to you or other users.

- [Comparing discovery and classification results](#)

Compare results from different runs of the same discovery and classification process.

- [Using the host references report](#)

The Host references report provides an easy way to identify where a server is used in Guardium and simplifies the process of decommissioning that server or updating its host name or IP address.

---

## Audit process task types

When you create an audit process with the Audit Process Builder, you need to select the database activity monitoring tasks to include in your audit process. Create the monitoring activities that you want to include before you start building the audit process.

### Process task types

---

An audit process can contain any number of audit tasks. Select the type of task from the New task window.

- Report - Produces a report, which can be either custom or a Guardium® predefined report. The report type must be Tabular.
- Security assessment - The security database assessment scans the database infrastructure for vulnerabilities, and provides an evaluation of database and data security health, with both real-time and historical measurements. The report compares the current environment against preconfigured vulnerability tests based on known flaws and vulnerabilities. The tests are grouped by using common database security best practices (like STIG and CIG1), as well as incorporating custom tests. The application generates a Security Health Report Card, with weighted metrics (based on best practices) and recommends action plans to help strengthen database security.
- Entity audit trail - Produces a detailed report of activity that relates to a specific entity is produced (for example, a client IP address or a group of addresses).
- Privacy set - Produces a report that details access to a group of object-field pairs (a Social Security number and a date of birth, for example) during a specified time period.
- Discover sensitive data - Scans the existing database metadata and data, reporting on information that might be sensitive, such as Social Security numbers or credit card numbers.
- External feed - Exports data to an external specialized application for further forensic analysis.

Note: The External Data Feed is an optional component that is enabled by a product key. This feature displays only if it is enabled.

Note: If data level security at the observed data level is enabled, then audit process output is filtered so that users see only the information of their databases.

### Defining a report task

---

Before you begin, you need a report. For more information about creating reports, see [Using the Query-Report Builder](#).

1. Select Report as the task type.
2. Enter a name for this task and select an existing report (which can be either a Guardium pre-defined or a user-defined report).
3. Select the format that you want for exporting: CSV, CEF, PDF, Write to Syslog, and Compress. For more information, see [Exporting audit results](#).
4. PDF options apply to both PDF attachments and PDF export files. If you select PDF, then you can further select from:
  - Report - The current results
  - Diff - The differences between a new report and the previous report (only available if a previous report exists)
  - Reports and Diff - Both the current and diff reports

Note: The maximum number of rows that can be compared at one time is 5000. If the number of result rows exceeds the maximum, an error message displays.

5. Enter all of the remaining information in the New task window. The information varies depending on the report that you select.

Note: When setting time periods, you can select Sync QUERY\_FROM\_DATE to the previous execution date to prevent missing or duplicate data in scheduled audit processes. If you select this option, be aware that:

- The audit process must run at least once before the setting takes effect.
- If an audit process has not run recently, consider disabling the setting to avoid an excessive amount of data in the report.

6. Click OK.

### Defining a security assessment task

---

Before you begin, you need a security assessment. For more information, see [Creating an assessment](#).

1. Select Security Assessment as the task type.
2. Enter a name for this task and select an existing security assessment.
3. Optionally, select whether to export the output in AXIS (Apache EXtensible Interaction System, used by QRadar) or SCAP (Security Content Automation Protocol) format.  
AXIS or SCAP saves the audit process results in XML format and transfers the file to the destination defined in Results Export. For more information, see [Exporting \(files\) results](#).
4. Select whether to create a PDF report that contains,
  - Report - The current results
  - Diff - The differences between a new report and the previous report (only available if a previous report exists)
  - Report and Diff - Both the current and diff reports

5. Click OK.

Note: If a security assessment task is empty (for example, a security assessment with a set of no roles), the empty security assessment does not display in the drop-down list in Audit Builder.

### Defining an entity audit trail task

---

1. Select Entity Audit Trail as the task type.
2. Enter a name for this task and then select the type of entity to audit. Depending on the entity that you select, supply the following information:
  - Object - Enter an object name.
  - Object Group - Select an object group from the list.
  - Client IP - Enter a client IP address.
  - Client Group IP - Select a client IP group.
  - Server IP - Enter a server IP address.
  - Application User Name - Enter an application user name.
3. Select whether to export the audit trail as a CSV file, and optionally, supply a label. For more information, see [Exporting output to CSV, CEF or PDF format](#).
4. Select whether to compress the audit trail.
5. In the Task Parameters section, supply runtime parameter values (Enter Period From and To are required).
6. Click OK.

## Defining a privacy set task

---

Before you begin, you need to create a privacy set. For more information, see [Privacy sets](#).

1. Select Privacy set as the task type.
2. Enter a name for this task and then select a privacy set from the Privacy Set list.
3. Select either Report by Access Details or Report by Application User to indicate how you want to sort and display the results.
4. Select whether to export the privacy set as a CSV file, and optionally, supply a label. For more information, see [Exporting output to CSV, CEF or PDF format](#).
5. Select whether to compress the privacy set.
6. Click OK.

## Defining a discover sensitive data task

---

Before you begin, you need to create a sensitive data scenario. For more information, see [Discover sensitive data](#).

1. Select Discover sensitive data as the task type.
2. Enter a name for this task and then select an existing sensitive data scenario from the Discover Sensitive Data list.
3. Click OK.

## External feed task

---

This type of task feeds data that is collected by Guardium to an external application, mapping the data to a format recognized by that application. External feed is an extra-cost feature, which is enabled by a patch.

If you use external feeds in a central manager environment, you must install the external feed patch on the central manager, and on all managed units on which the task runs. For more information, see [Working with external feeds](#). For more information about how the data is mapped from Guardium to an external application, see the documentation for the purchased option.

1. Select External Feed as the task type.
2. Enter an name for this task and then enter the following options:
  - Select a feed type from the Feed Type list
  - Select an External Feed event
  - Select a report from the Report list. Depending on the report selected, additional parameters display.
  - Under Extract Lag, enter the number of hours by which the feed is to lag, or select Continuous to include data up to the time that the audit task runs.
  - Select one or more datasources for the external feed. If needed, click the  icon to create a new datasource.
3. Click OK.

## Using APIs to automate audit process runs

---

By default, some reports are linked to API functions. You can use these API calls to run for every record within a task of type report in an audit process. You can also add API mapping to a report by right-clicking in the report row, select Add API mapping, and selecting the API function in the Add API Mapping window. To configure an API for automatic execution for a report task:

1. From the Report task, select a report for which API for automatic execution displays, such as the Guardium Group Details, Job Dependencies, or Restored Data reports.
2. From API for automatic execution select an API from the list.
3. Click Event and Additional Columns. The Event, Sign-off & Additional Column window opens.
4. Under Define Additional Columns, in the Column Name, type API\_RESULT\_TEXT.
5. In the Type column, select Text.
6. Click Add.
7. Run the audit process and click View Results. The API\_RESULT\_TEXT column has the returned text, and the BY column has the name of the API ran, and the date and time when it was run.

## Audit process receivers

---

Use the audit process builder to send audit process output to many different people or groups (receivers). These process receivers can view and manage audit process output.

Audit process receivers are notified via email or their To-Do list of pending audit process results. You can designate any receiver as a signer for a process. In this case, the results can be held at that point on the distribution list until that receiver electronically signs the results or releases them.

You can define any number of receivers for a workflow automation process, and you control the order in which they receive results. In addition, receivers can notify other receivers, using the Escalate function. It is also possible to run an audit process with no defined receivers. For example, you can create an audit process with no receivers

that writes to syslog and has no need to review (or sign) the results.

## Adding receivers

---

From the Audit Process Builder,

1. Open the Send results ribbon and then click  to open the New Receiver window.
2. From the New Receiver window, select a Receiver type, which can be one of the following:
  - Role - Select a role from the Role list. Guardium sends results to all users with the specified role.
  - Email - Specify an address in Email address. Guardium sends results to the specified email address. In addition, you can select the following options:
    - Email format - Choose whether to send results as a PDF or in CSV format.
    - Approve if empty - Automatically approve this report if no results are returned.
    - Do not include online links to reports in email - Remove links to online reports from the notification email. Select this option if the receiver might not have access to Guardium system.
  - User Group - Select or create a new user group in the Group list. Guardium sends results to all users that are members of the group.
  - User - Select a user from the User list or click Search Users to find a user to add. Guardium sends results to the specified user.
3. Ticket- Click  to begin searching for either a user or group to whom to assign this ticket.
  - From the Search Users or Search Groups window, enter the name of the user or group.
  - Click Search.
  - Select a user or group, then click Add.

Guardium assigns the ticket to the specified user or group.

3. For Role, User Group, and User receivers, you can set the following options:

- Action - Select any of the following actions:
    - Review - The receiver does not need to sign the results.
    - Sign off - The receiver must sign the results (electronically, by clicking Sign Results when viewing the results online). For user groups, if Sign off is selected, all members of the group must sign.
    - Approve if empty - Automatically approve this report if no results are returned.
    - Add to to-do list - Send a notice of to the user's audit process to-do list. For more information, see [Audit Process To-Do List](#).
  - Email format - Select an email format:
    - None - Do not send email to the receiver.
    - Links only - Include hypertext links to the results (on the Guardium system).
    - Full results - Include a copy of the results in PDF or CSV format.
- Note: Results from Security Assessment or Discover Sensitive Data tasks might return sensitive information.
3. Distribution sequence - Select whether audit process results are sent to all receivers at the same time (Simultaneous) or only after the previous receiver reviews or signs off on the results (Sequential).

## Receiver details

---

When you select Role or User Group as a receiver, all users that belong to the group or having that role receive the results.

If you select a group receiver, and any workflow automation task uses the special runtime parameter `./LoggedUser` in a query condition, then the query executes separately for each user in the group, and each user receives only their results.

For example, assume that your company has three DBAs, and each DBA is in charge of a different set of servers. You use the Custom Data Upload facility to upload the areas of responsibilities of each DBA (with server IPs) to the Guardium® system. You can correlate that to the database activity domain, and then use a report in this custom domain as an audit task. If a user group that contains the three DBAs is designated as the receiver, each DBA receives the report relevant only for their collection of servers.

If you specify a group receiver and require sign-off, each member of the group must sign the results separately (as explained earlier, each member of the group may be looking at a different set of results).

If you select Email as the receiver, the results are sent to the specified email address. When you specify an email address, that address that is used to filter the data. The email address must belong to a user who is logged in or is under the user in the data hierarchy.

If you specify a role receiver, only one user with that role needs to sign the results. The other users with that role are notified when the results are signed.

Note: Be sure to configure audit processes so that all roles that act on an event associated with an audit process are receivers of that audit process. When you create a workflow event, you can assign a role to every status that is used by that event (that is, users with that role can only see events when the event is in the specified status). When you assign an event to an audit process, it is important that every role that is assigned to a status of this event have a receiver on this audit process. Otherwise, an audit result row can end up with a status where none of its receivers are able to see this row or change its status.

If this situation occurs, the admin user (who can see all events, regardless of their roles) can see the row and change its status. However, if data level security is on, the admin user might not be able to see this row. In this case, the admin user must either turn off data level security (from Global Profile) or have the dataset\_exempt role.

## Hypertext links to process results

---

In email messages, there are conditions where links to process results on the Guardium system will not work. For example:

- If you access email from a location where you cannot normally access the Guardium system, the links do not work. For example, if you are on your personal computer, you might have access to your email over the Internet, but not to your company's private network or LAN, where the system is installed.
- If you have not accessed your email for a longer period of time than the report results are kept, those results are not available when you click the link. For example, if results are kept for seven days, and you take a two week vacation, your email may contain links to results older than seven days, and those links will not work.

## Modifying the receivers list after an audit process runs

---

After an audit process runs, any user can add, edit, delete, and rearrange receivers on the receivers list. From the Audit Process Builder, select an active audit process and open its Send results ribbon:

- Click , , or to add, edit, or delete receivers.
- Click to enable the reorder controls and change the position of receivers in the list.

Changes to the receivers list are tracked in the User Activity Audit Trail report. From the report, right-click an UPDATE activity type, select Detailed Guardium user activity, and look for Audit process entries under the Modified entity column.

Note:

If you delete the Guardium user account for a receiver on the list, Guardium substitutes the admin user account (which is never deleted) for that receiver. In this case, the admin user receives any email notifications that are sent to a deleted receiver, and the admin user must act upon any results released to that receiver.

## How results are released to receivers

---

Results are released to the Guardium users listed on the receivers list, subject to the Continuous check box, as follows:

- If the Continuous check box is marked, distribution continues to the next receiver on the list without interruption.
- If the Continuous check box is cleared, distribution to the next receiver is held until the current receiver performs the required action (review or sign).

For example, assume you want to define a workflow process for DBAs:

- All DBAs should receive their results at the same time, with each DBA receiving a different result set based on the server IPs with which they are associated.
- Only when ALL DBAs have signed, the DBA Manager should see the results.
- Only when DBA Manager releases the report, the Auditors should see the results.
- All Auditors should receive the reports at the same time, but only one of them (any of them) needs to sign each result. The others will be updated when a result was signed.
- An auditor can escalate a result to the Audit Manager.

To define this flow:

- The DBAs group would be named as the first receiver.
- The DBA Manager would be next on the list.
- The Auditors role (not group) would be next on the list. Any Auditor could sign and others will be notified. Also, any auditor can escalate a results set to the Audit Manager.

Note: The results will only distribute to the next receiver when the current receiver has marked the Continuous button. This is completely separate from the review/sign functionality and does not depend on the review/sign functionality all.

Note: Process results that are exported to CSV or CEF files are sent to another network location by the Guardium archiving and exporting mechanism. These results are not subject to the receivers list or to any signing actions. They are subject to the Guardium CSV/CEF export schedule (if any is defined), and they are subject to the access permissions that have been granted for the directory in which they are ultimately stored.

## View or sign results

---

- Open the Compliance Workflow Automation results.
- If signing is required, click the Sign Results button.
- Optional. To forward these results to another user, click Escalate, and see Forward Results to Additional Receivers (in Escalation section).
- Click Close this window link.

Note: If there are outstanding events, then the results cannot be signed either from the audit viewer or from the To-do list. If there are outstanding events and an attempt is made to sign the results, the following message appears:

**Audit process cannot be signed - has pending events.**

**Please update all outstanding events prior to signing this result.**

Note: When viewing audit process results, if a result has events associated with it, the Sign Results button is not available on this result until all events are in a Final state or cannot be seen by this user (due to data-level security).

Note: This report also contains a date or Last Action Time, located in a column between Receiver and Status. This report shows that the result was signed by user AAA, but also when this user AAA signed this result.

## Release results without signing or viewing

---

- Open your To-Do List panel.
- Click the Continue button for the results you want to release to the next receiver on the distribution list.
- Click Close this window link.

## View Results Distribution

---

- Open the compliance workflow automation results.
- Expand the Distribution Status panel by clicking the (Show Details) button.
- Click Close this window link.

## View receiver comments added to results

---

- Open the compliance workflow automation results.
  - Expand the Comments panel by clicking the Show Details button.
- Note: These are the comments that were attached to the results when the report page was retrieved from the Guardium system. If you add comments of your own, or if other receivers are adding comments simultaneously, you will not see those comments until you refresh your page (using your browser Refresh function).

- Click Close this window link.

## Escalate process results

---

A receiver of process results can forward the results notification for review and/or sign-off to additional receivers. If you escalate the results to a receiver outside of the original audit and sign-off trail, and the results include a CSV file, that file will not be included with the notification.

Regardless of who is a receiver of an audit result, an escalation can involve any user on the system, provided the Escalate result to all users box is checked in the Setup > Tools and Views > Global Profile menu. A check mark in this box escalates audit process results to all users, even if data level security at the observed data level is enabled. The default setting is enabled. If the check box is disabled (no check mark in the check box), then audit process escalation will only be allowed to users at a higher level in the user hierarchy. If the check box is disabled, and there is no user hierarchy, then no escalation is permitted.

Also, depending on event permissions, if for example, the infosec user can only see events in status1 and dba user can only see events in status2, the dba user will receive a different result than the result the infosec user saw when the infosec user clicked Escalate. It is possible that infosec will escalate to dba, and dba will receive an audit result with 0 rows in it.

1. If the compliance workflow automation results you want to forward are not open, open them now.
2. Click Escalate.
3. Select the receiver from the Receiver list.
4. In the Action Required column, select Review (the default) or Review and Sign.
5. Click the Escalation button to complete the operation.

Note: Audit process results cannot be escalated to a group of users, only to users or roles.

When escalating to a user who already has the result in the user's to-do list, a popup message will appear, asking if an additional email should be sent. If yes, an additional email will be sent to the user, but the to-do list will not be incremented.

## Exporting audit results

Reports that contain information that can be used by other applications, or reports that contain large amounts of data, can be exported to other file formats.

### Exporting output to CSV, CEF or PDF format

You can export report, entity audit trail, and privacy task output to CSV files, and export database activity reports to a CEF file. When exporting to CEF or CSV files, keep in mind the following details,

- Each record in the CSV or CEF file represents a row on the report.
- CEF and CSV file output can be written to syslog. If the remote syslog capability is used, this results in the immediate forwarding of the output CEF or CSV file to the remote syslog locations. You can use the remote syslog function to direct messages from each facility and severity combination to a specific remote system. For more information, see [Facility and priority of syslog messages](#). For more information about the remotelog (syslog) CLI command, see [store remotelog](#)
- Guardium creates the file to export in addition to the standard task output, but does not replace it. Exporting the files can be useful for the following tasks,
  - Integrating with an existing SIEM (Security Incident and Event Manager) in your infrastructure (such as QRadar, ArcSight, Network Intelligence, LogLogic, or TSIEM).
  - Reviewing and analyzing very large compliance task results sets. Results sets exported to PDF are limited to 5,000 rows of output. There is no limit to the number of rows that can be written to an exported CSV or CEF file when using an audit process.
- Exported CSV and CEF files are stored on the Guardium® system, and are named in the format:

`process_task_YYYY_MM_DD-HHMMSS.<csv | cef>`

Where `process` is the process name and `task` is the task name that you defined for this audit process. The date-time stamp is generated when the task runs.

- You cannot access the exported CSV or CEF files directly on the Guardium system. Your Guardium administrator must use the CSV/CEF Export function to move these files from the Guardium system to another location on the network. To access those files, check with your Guardium administrator to determine their location. The fact that exported files are sent outside of the Guardium system has two important implications:
  - The release of these files is not connected to the results distribution plan defined for the audit process. These files are exported on a schedule defined by the Guardium administrator.
  - Once the CSV/CEF Export function runs, all exported files will be available to anybody (Guardium user or not) who can access the destination directory defined for the CSV/CEF Export operation. For this reason, your Guardium administrator may want to schedule additional jobs (outside of the Guardium system) to copy sets of exported files from the Guardium CSV/CEF Export destination directory, to directories with appropriate access permissions.

- CSV/CEF Export activity is available in the Aggregation/Archive Activity report.

Note: If observed data level security is enabled, then audit process output (including files) is filtered so users will see only the information for their assigned databases. Files sent to an email receiver as an attachment will be filtered. However, files downloaded locally on the machine and then moved elsewhere using the Results Export function are not subject to data level security filtering.

The following table summarizes what happens when an audit process file is exported to CSV, CEF, or PDF.

Table 1. Exporting Audit Task Output to CSV, CEF or PDF Files

| Function                                | Level         | CSV                                                                                   | CEF                                                                                   | PDF                                                                                   |
|-----------------------------------------|---------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Attach to email                         | Receiver      | Full Details radio --> PDF check box                                                  | N/A                                                                                   | Full Details radio --> PDF check box<br>The radio buttons are only for receiver PDF   |
| Export file                             | Task          | Export CSV file check box                                                             | Export CSV file check box                                                             | Export CSV file check box                                                             |
| Report empty and Approve if Empty = yes | Receiver      | Export not affected (empty files will be exported)<br>Attachment, no email attachment | Export not affected (empty files will be exported)<br>Attachment, no email attachment | Export not affected (empty files will be exported)<br>Attachment, no email attachment |
| Zip attachment                          | Audit Process | If no file generated, nothing to zip<br>Merge all CSVs into one ZIP file              | N/A                                                                                   | If no file generated, nothing to zip<br>PDF is not zipped                             |
| Compress (export)                       | Task          | Compressed, separate file for each CSV file                                           | Compressed, separate file for each CSV file                                           | PDF is not compressed                                                                 |

## How zip for email and compress work for audit task output

---

Zip for email is the highest level of control for Audit Task Export. Zip for email produces a set of CSV or CEF files. PDFs are never zipped or compressed.

Compress works on individual files.

Note: For CSV attachments, when Zip for Email is cleared, Compress can still be applied. And Compress can be per task. Thus one Audit Task may send a .csv file while another may send a .csv.gz file, in the same email.

The interaction of Zip for Email and Compress is as follows:

- Zip for email checked (regardless of whether Compress is also checked), the attachment is one zip file of CSV files.
- Zip for email not checked, and Compress checked, the attachment is a set of csv.gz files.
- Zip for email not checked, and Compress not checked, the attachment is a set of CSV files.
- Compress checked, Download All will be csv.gz.
- Compress cleared, Download All will be csv.
- Compress checked or cleared, download displayed will still be CSV.
- Compress checked, export of CSV/CEF files will be gzipped.
- Compress cleared, export of CSV/CEF files will not be gzipped.

---

## How to distribute workflow through Guardium groups

Using the receiver group option, define a single Compliance Workflow audit process that will send different results to different Guardium users based on a pre-defined, custom mapping.

Value-added: Setup a single audit process and distribute the appropriate results to the appropriate manager. This saves having to create separate audit processes for separate receivers.

IBM® Guardium®'s Compliance Workflow Automation automatically delivers reports, classification results, and security assessment results to Guardium users on a scheduled basis. Result receivers can be defined as Guardium users, Guardium roles or user groups.

For example, consider a large organization that has fifteen DBA managers that need to review the activities for the DBAs they manage without viewing the activities of the other manager's DBAs. One solution would be to setup fifteen separate audit processes; one for each manager. This would take a lot of time to configure and it is difficult to manage: Each audit process needs to be scheduled separately and any global change would need to be made individually for all fifteen audit processes.

The user group distribution method, on the other hand, permits the setup of a single audit process and distributes the appropriate results to each manager based on a manager/DBA mapping. This process requires more upfront configuration but reduces to maintenance time. Only one audit process needs to be scheduled and changes only need to be applied in one location.

## User mapping

---

The first step in the process is to map the users to the data elements within Guardium that will be the basis for report distribution. The example that will be used in this document will be based on objects, but you can apply these concepts with any data element within Guardium.

Example: Three users have responsibility over three different sets of tables, based on audit requirements (PCI, HIPPA, and CCI) within a database server, as follows:

Table 1. User with Table/Object

| User   | Table/Object         |
|--------|----------------------|
| User01 | db2inst1.cc_numbers  |
| User01 | db2inst1.ccn         |
| User02 | db2inst1.ADDRESSES   |
| User02 | db2inst1.SSN_NUMBERS |
| User02 | db2inst1.G_CUSTOMERS |
| User02 | db2inst1.G_EMPLOYEES |
| User02 | db2inst1.G_FUNDS     |
| User03 | db2inst1.doctor      |
| User03 | db2inst1.medicare    |
| User03 | db2inst1.med_history |

This table must be added as a custom table within Guardium, either manually or through a data upload. The following steps demonstrate how to create a custom table manually. The screenshots are from the "admin" user interface, but they can also be accessed from within the "user" user interface.

1. Navigate to Reports > Report Configuration Tools > Custom Table Builder and press the **Manually Define** button.

2. At the **Custom Table Builder** screen, define the table layout. Make sure that **Group Type** matches the correct data element in Guardium. Press **Apply** and **Back** when complete.

3. Press **Edit Data** to manually add the records. Note, if you have a large amount of data, choose **Upload Data** to import from an external data source.

4. Press **Insert**.

5. Enter each combination of values and press **Insert** until you have added all of the required records.

Custom Table Builder

**Custom Data - Insert Record**

Table: ObjectUserMapping Entity: ObjectUserMapping

- Leave a field blank to not specify a value for the column.  
 - Use 'guardium://empty' to specify an empty value.  
 - Use 'guardium://null' to specify the value NULL.

|                        |                     |
|------------------------|---------------------|
| User - Text(255)       | User01              |
| SensObject - Text(255) | db2inst1.cc_numbers |

Cancel **Insert**

6. When complete, press the **Query** button to review the data.

Custom Table Builder

**Custom Data Editor**

Table: ObjectUserMapping Entity: ObjectUserMapping

There are currently 10 row(s) in this table. **Insert...**

Query rows to view, update, or delete:

| Column     | Type | Size | Filter (optional) |
|------------|------|------|-------------------|
| User       | Text | 255  |                   |
| SensObject | Text | 255  |                   |

- Leave Filter blank to omit criteria for a column  
 - Use 'guardium://empty' to specify an empty value.  
 - Use 'guardium://null' to specify the value NULL.  
 - All other comparisons use LIKE and accept the '%' wildcard

**Query** **Back**

7. Press return when complete.

Custom Table Builder

**Queried Records**

Table ObjectUserMapping  
 Entity ObjectUserMapping

| Select All                        | Unselect All | Delete               |
|-----------------------------------|--------------|----------------------|
| Datasource                        | User         | SensObject           |
| <input type="checkbox"/> [MANUAL] | User01       | db2inst1.cc_numbers  |
| <input type="checkbox"/> [MANUAL] | User01       | db2inst1.ccn         |
| <input type="checkbox"/> [MANUAL] | User02       | db2inst1.ADDRESSES   |
| <input type="checkbox"/> [MANUAL] | User02       | db2inst1.SSN_NUMBERS |
| <input type="checkbox"/> [MANUAL] | User02       | db2inst1.G_CUSTOMERS |
| <input type="checkbox"/> [MANUAL] | User02       | db2inst1.G_EMPLOYEES |
| <input type="checkbox"/> [MANUAL] | User02       | db2inst1.G_FUNDS     |
| <input type="checkbox"/> [MANUAL] | User03       | db2inst1.doctor      |
| <input type="checkbox"/> [MANUAL] | User03       | db2inst1.medicare    |
| <input type="checkbox"/> [MANUAL] | User03       | db2inst1.med_history |

1 to 10 of 10 **Return**

## Custom Domains

Next, join this custom table to the Guardium table structure using Custom Domains.

1. Navigate to Reports > Report Configuration Tools > Custom Domain Builder. Highlight *[Custom]* Access and press **Clone**.

The screenshot shows the IBM Guardium Data Protection interface. The top navigation bar includes 'System View', 'Administration Console', 'Tools' (with a dropdown arrow), 'Daily Monitor', 'Guardium Monitor', 'Tap Monitor', 'Incident Management', and 'Reports'. Under 'Tools', 'Custom Domain Builder' is selected. On the left, a sidebar lists various tracking categories like 'Access Tracking', 'Report Building', and 'Custom Domain Builder'. The main panel is titled 'Domain Finder' and contains a list of domain entities such as 'S-TAP Info', 'STAP Association History', 'SYBASE: Accnts With Sys Or Sec Admin Roles', etc. A red box highlights the 'Custom Domain Builder' option in the sidebar and the 'Object' entity in the list.

2. In the Custom Domain Builder:

- Highlight the new table created under **Available entities**.
- Highlight the table under **Domain entities** to which you would like to join the custom table.
- Under **Join condition** choose the fields on each table on which to create the join and press **Add Pair**.

This screenshot shows the 'Custom Domain Builder' dialog. The 'Custom Tables Domain' section has a 'Domain name' of '-ObjectUserMapping01'. The 'Available entities' pane on the left lists various MySQL and Netezza privilege tables. The 'Domain entities' pane on the right lists domain entities like 'Access Period', 'Session', 'Client/Server', 'SQL', 'Command', and 'Object'. The 'Object' entity is highlighted with a red box. The 'Join condition' section at the bottom shows a pair 'SensObject' = 'Object Name' selected with a red box. Buttons for 'Delete All Pairs', 'Add Pair', 'Apply', and 'Back' are visible.

3. Press the arrows (>>) button to move the custom table from **Available entities** to **Domain entities**.

This screenshot shows the 'Custom Domain Builder' dialog after pressing the '>>' button. The 'Available entities' pane now shows the '-ObjectUserMapping' table moved to the 'Domain entities' pane. The 'Domain entities' pane still contains the 'Object' entity. The 'Join condition' section remains the same as in the previous screenshot.

4. Press the **Detail** button to review the joins.

Custom Domain Builder

**Custom Tables Domain**

Domain name: -ObjectUserMapping01  
Timestamp Attribute: Access Period Period Start

**Available entities**

- ClassificationDataImport
- CM Buffer Usage Monitor
- DB2 Column Level Prvls
- DB2 DB Level Prvls
- DB2 Index Level Prvls
- DB2 Package Level Prvls
- DB2 Priv Summary
- DB2 Table Level Prvls
- Enterprise No Traffic
- Enterprise S-TAPs Changed
- Informix Account With Dba Privilege
- Informix Execute Priv On Proc Func To Public

**Domain entities**

- Access Period
- Session
- Client/Server
- SQL
- Command
- Object**
- Field
- FULL SQL
- Application Events
- ObjectUserMapping**

**Join condition**

To add an entity to a non-empty domain, select an available entity and attribute, select a domain entity and attribute, click the add button above.

SensObject = Object Name

Detail

Delete All Pairs Add Pair Apply Add Comments Back

5. Confirm that the joins are correct and press **Close**.



6. Press **Apply** to save the new custom domain.

Custom Domain Builder

**Custom Tables Domain**

Domain name: -ObjectUserMapping01  
Timestamp Attribute: Access Period Period Start

**Available entities**

- ClassificationDataImport
- CM Buffer Usage Monitor
- DB2 Column Level Prvls
- DB2 DB Level Prvls
- DB2 Index Level Prvls
- DB2 Package Level Prvls
- DB2 Priv Summary
- DB2 Table Level Prvls
- Enterprise No Traffic
- Enterprise S-TAPs Changed
- Informix Account With Dba Privilege
- Informix Execute Priv On Proc Func To Public

**Domain entities**

- Access Period
- Session
- Client/Server
- SQL
- Command
- Object**
- Field
- FULL SQL
- Application Events
- ObjectUserMapping**

**Join condition**

To add an entity to a non-empty domain, select an available entity and attribute, select a domain entity and attribute, click the add button above.

SensObject = Object Name

Detail

Delete All Pairs Add Pair **Apply** Add Comments Back

## Custom Report

Next, create a report to distribute to the users.

1. Navigate to Reports > Report Configuration Tools > Report Builder and select the new domain from the Domain drop-down menu.

The screenshot shows the 'Custom Query Builder' interface with the 'Domain Finder' search results. The search term '-ObjectUserMapping01' is entered in the search bar, and the results list various database objects and privileges. A red box highlights the 'Search' button at the bottom right of the search results panel.

2. Press **New...**

The screenshot shows the 'Query Finder' section of the 'Custom Query Builder'. It includes fields for 'Query Name', 'Report Title', and 'Main Entity', each with dropdown menus. A red box highlights the 'New...' button at the bottom right.

3. Enter a **Query Name** and **Main Entity** and press **Next**.

The screenshot shows the 'New Query - Overall Details' step. The 'Query Name' field is set to '-ObjectUserMapping01' and the 'Main Entity' field is set to 'Object'. A red box highlights the 'Next' button at the bottom right.

4. Create a new report with a run-time parameter for the user field created in the custom table.

The screenshot shows the 'ObjectUserMapping01' query configuration screen. The 'Query Fields' table has the following data:

| Seq. | Entity        | Attribute    | Field Mode | Order by | Sort Rank | Descend |
|------|---------------|--------------|------------|----------|-----------|---------|
| 1    | Client/Server | Server IP    | Value      |          |           |         |
| 2    | Client/Server | Client IP    | Value      |          |           |         |
| 3    | Client/Server | DB User Name | Value      |          |           |         |
| 4    | Command       | SQL Verb     | Value      |          |           |         |
| 5    | Object        | Object Name  | Value      |          |           |         |

The 'Query Conditions' section contains the following WHERE clause:

```

WHERE ObjectUserMapping = User = (Parameter) LoggedUser

```

The 'Runtime Params.' dropdown is set to 'LoggedUser'. A red box highlights the 'Generate Tabular' button at the bottom left.

## User Group

Create a new group of “Guardium Users” based on the custom table.

1. Navigate to Setup>Tools and Views>Group Builder and create a new group with **Guardium Users** as the **Group Type**.

The screenshot shows the 'Group Builder' tool within a larger application interface. The top navigation bar includes 'System View', 'Administration Console', 'Tools' (with a gear icon), 'Daily Monitor', 'Guardium Monitor', 'Tap Monitor', 'Incident Management', and 'Reports'. The left sidebar lists various builders: Access Map Builder/Viewer, Alert Builder, Alias Builder, Audit Process Builder, Audit Process To-do List, Auto-discovery Configuration, Baseline Builder, CAS Host Config, CAS Template Set Config, Classification Policy Builder, Classification Process Builder, Datasource Definitions, Group Builder (which is selected and highlighted with a red box), Policy Builder, Portlet Editor, Privacy Set Builder, Replay Builder, Security Assessment Builder, Time Period Builder, Value Change Audit DB Creation, Value Change Audit DB Update & Upload, Value Change Auditing Builder, and Workflow Builder.

The main panel displays the 'Group Builder' interface. It includes a 'Modify Existing Groups' section with a list of items such as 'App Users', 'Application Servers', 'Customer Tables', 'Allowed Connections', 'appservers', 'DBAs', 'IBM Citrix IPs', 'IBM DBAs', and 'Non-system tables'. Below this are buttons for 'Auto Generated Calling Prox', 'Populate from Query', 'LDAP', 'Group Filter', 'Roles...', 'Clone', 'Modify', and 'Delete'. A section titled 'Flatten All Hierarchical Groups Scheduling' indicates that flattening is not scheduled, with buttons for 'Modify Schedule...' and 'Run Once Now'.

The 'Create New Group' section is highlighted with a red box. It contains fields for 'Application Type' (set to 'Public'), 'Group Description' (set to '-ObjectUser'), 'Group Type Description' (set to 'Guardium Users'), 'Group Sub Type Description' (with 'Category' and 'Classification' fields), and a 'Hierarchical' checkbox. A large 'Add' button is located at the bottom right of this section.

2. Add all of the users from the custom table.

This screenshot shows the 'Manage Members for Selected Group' dialog box. At the top, it displays the 'Group Name' as '-ObjectUser' and the 'Group Type' as 'Guardium Users'. It includes buttons for 'Modify Group Type' and 'Modify Category'. The main area is titled 'Group Members' and features a 'Filter' input field and a list of members: 'user01', 'user02', 'user03', and 'user04'. These four entries are highlighted with a red box. Below the list, there are three sections: 'Create & add a new Member named' with a text input 'user05' and an 'Add' button; 'Rename selected Member to' with a text input and an 'Update' button; and 'Delete selected Member' with a 'Delete' button. At the bottom are buttons for 'Add Comments', 'Aliases...', 'LDAP', and 'Back'.

## Audit Process

1. Create a new Audit Process.
2. Choose the group created in User Group as the **Receiver**
3. Choose the custom report created in step 4 as the task.
4. In the run-time parameter, enter the special tag "./LoggedUser". This will cause the results to be distributed based on the custom mapping.
5. Press **Run Once Now** to run the Audit Process

When the audit process completes, each receiver should a different result set based the mapping:

## Users

User01

| Report details: |               |              |             |                                                                |                                                       |                                   |
|-----------------|---------------|--------------|-------------|----------------------------------------------------------------|-------------------------------------------------------|-----------------------------------|
|                 |               |              |             | <input checked="" type="checkbox"/> Compare with other results | <input checked="" type="radio"/> Show original values | <input type="radio"/> Use Aliases |
| Server IP       | Client IP     | DB User Name | SQL Verb    | Object Name                                                    | Count of Objects                                      |                                   |
| 192.168.169.7   | 192.168.169.7 | A2840        | CREATE VIEW | db2inst1.cc_numbers                                            | 1                                                     |                                   |
| 192.168.169.7   | 192.168.169.7 | A2840        | SELECT      | db2inst1.cc_numbers                                            | 1                                                     |                                   |
| 192.168.169.7   | 192.168.169.7 | ASEVIN       | CREATE VIEW | db2inst1.cc_numbers                                            | 1                                                     |                                   |
| 192.168.169.7   | 192.168.169.7 | ASEVIN       | SELECT      | db2inst1.cc_numbers                                            | 1                                                     |                                   |
| 192.168.169.7   | 192.168.169.7 | DB2INST1     | DROP TABLE  | db2inst1.CCN                                                   | 1                                                     |                                   |
| 192.168.169.7   | 192.168.169.7 | DB2INST1     | DROP TABLE  | db2inst1.CC_NUMBERS                                            | 1                                                     |                                   |
| 192.168.169.7   | 192.168.169.7 | KTRIMPE      | SELECT      | db2inst1.ccn                                                   | 1                                                     |                                   |
| 192.168.169.7   | 192.168.169.7 | KTRIMPE      | SELECT      | db2inst1.cc_numbers                                            | 1                                                     |                                   |
| 192.168.169.7   | 192.168.169.7 | SCOTT        | SELECT      | db2inst1.ccn                                                   | 1                                                     |                                   |
| 192.168.169.7   | 192.168.169.7 | SCOTT        | SELECT      | db2inst1.cc_numbers                                            | 1                                                     |                                   |

User02

Report Parameters used:

QUERY\_FROM\_DATE: 10/25/11 4:10 PM  
 QUERY\_TO\_DATE: 10/26/11 4:10 PM  
 LoggedUser: JLoggedUser  
 REMOTE\_SOURCE:

Report details:  Compare with other results  Show original values  Use Aliases

| Server IP     | Client IP     | DB User Name | SQL Verb         | Object Name          | Count of Objects |
|---------------|---------------|--------------|------------------|----------------------|------------------|
| 192.168.169.7 | 192.168.169.7 | A4939        | BEGIN            | db2inst1.g_customers | 2                |
| 192.168.169.7 | 192.168.169.7 | A4939        | CREATE PROCEDURE | db2inst1.g_customers | 2                |
| 192.168.169.7 | 192.168.169.7 | A4939        | INSERT           | db2inst1.g_customers | 2                |
| 192.168.169.7 | 192.168.169.7 | A4939        | REVOKE           | db2inst1.g_employees | 1                |
| 192.168.169.7 | 192.168.169.7 | A8000        | INSERT           | db2inst1.G_EMPLOYEES | 1                |
| 192.168.169.7 | 192.168.169.7 | A8000        | SELECT           | db2inst1.g_employees | 1                |
| 192.168.169.7 | 192.168.169.7 | A9404        | BEGIN            | db2inst1.g_customers | 1                |
| 192.168.169.7 | 192.168.169.7 | A9404        | CREATE PROCEDURE | db2inst1.g_customers | 1                |
| 192.168.169.7 | 192.168.169.7 | A9404        | GRANT            | db2inst1.g_employees | 1                |
| 192.168.169.7 | 192.168.169.7 | A9404        | INSERT           | db2inst1.g_customers | 1                |
| 192.168.169.7 | 192.168.169.7 | AMAZON       | INSERT           | db2inst1.G_EMPLOYEES | 1                |
| 192.168.169.7 | 192.168.169.7 | AMAZON       | SELECT           | db2inst1.g_employees | 1                |
| 192.168.169.7 | 192.168.169.7 | CHENSLER     | GRANT            | db2inst1.g_employees | 1                |
| 192.168.169.7 | 192.168.169.7 | DB2INST1     | DROP TABLE       | db2inst1.ADDRESSES   | 1                |
| 192.168.169.7 | 192.168.169.7 | DB2INST1     | DROP TABLE       | db2inst1.G_CUSTOMERS | 1                |
| 192.168.169.7 | 192.168.169.7 | DB2INST1     | DROP TABLE       | db2inst1.G_EMPLOYEES | 1                |
| 192.168.169.7 | 192.168.169.7 | DB2INST1     | DROP TABLE       | db2inst1.G_FUNDS     | 1                |
| 192.168.169.7 | 192.168.169.7 | DB2INST1     | DROP TABLE       | db2inst1.SSN_NUMBERS | 1                |
| 192.168.169.7 | 192.168.169.7 | KJAIN        | BEGIN            | db2inst1.g_customers | 1                |
| 192.168.169.7 | 192.168.169.7 | KJAIN        | CREATE PROCEDURE | db2inst1.g_customers | 1                |

Records: 1 To 20 Of 22

User03

Report Parameters used:

QUERY\_FROM\_DATE: 10/25/11 4:10 PM  
 QUERY\_TO\_DATE: 10/26/11 4:10 PM  
 LoggedUser: JLoggedUser  
 REMOTE\_SOURCE:

Report details:  Compare with other results  Show original values  Use Aliases

| Server IP     | Client IP     | DB User Name | SQL Verb   | Object Name          | Count of Objects |
|---------------|---------------|--------------|------------|----------------------|------------------|
| 192.168.169.7 | 192.168.169.7 | AMAZON       | INSERT     | db2inst1.doctor      | 1                |
| 192.168.169.7 | 192.168.169.7 | ASEVIN       | INSERT     | db2inst1.doctor      | 1                |
| 192.168.169.7 | 192.168.169.7 | DB2INST1     | DROP TABLE | db2inst1.doctor      | 1                |
| 192.168.169.7 | 192.168.169.7 | DB2INST1     | DROP TABLE | db2inst1.medicare    | 1                |
| 192.168.169.7 | 192.168.169.7 | DB2INST1     | DROP TABLE | db2inst1.med_history | 1                |

Records: 1 To 5 Of 5

## Audit Process To-Do List

Use the Audit Process To-Do List to track tasks that are assigned to you or other users.

As an administrator, you can perform any actions on any to-do list entry. Any actions that you take are logged, indicating that the action was taken by the administrator on behalf of the user. You can manage audit processes one at a time or in bulk. For more information, see Step 3.

- Open the Audit Process To-Do List by one of:

- Click the icon in the page banner.
- Browse to Comply > Tools and Views > Audit Process To-Do List.
- If you receive an email notification, click the To-Do List link to open your To-Do List. Alternatively, click the report link to open the results. In either case, you must have access to your email from a location that also has access to Guardium®.

- Take one of the following steps to filter the list:

- Select the user whose To-Do list you want to open, either from View To-Do List of, or click Search Users and select a Role or User from the Search Users dialog.
- Type in part or all of a Process name and click Search.
- Select either an Execution start date, an Execution end date, or both.

- Within the processes list, you can mark multiple processes as viewed or signed. To work with multiple processes:

- Select one or more processes from the list and click Mark selected as viewed to change each process to viewed. When prompted, add a comment and then click Add comment. The comment is the same for all selected processes.

- If you have signing authority, you can then click Mark selected as signed to mark each selected process as signed. When prompted, add a comment and then click Add comment.

If you select Apply to all processes with selected name, and then click Mark selected as viewed or Mark selected as signed, Guardium performs the requested action on all processes with the selected name.

For example, say the **Process1** process runs every 10 minutes. You usually turn it off at night, but you forgot and when you come in the next morning, multiple pages of **Process1** audit processes are waiting in your To-Do list. Rather than opening each **Process1** process, you can take the following steps:

- a. Select **Process1** from the list and select Apply to all processes with selected name. All processes named **Process1** are selected, even if they are not on the visible page.
- b. Click Mark selected as viewed.
- c. Enter a comment and click Add comment.
- d. All of the **Process1** processes in your list are now marked as viewed. If you have signing authority, then Sign viewed results displays for each process.
- e. If you have signing authority, you can now select a process again, and select Apply to all processes with selected name.
- f. Then, click Mark selected as signed, enter a comment, and click Add comment.

Note: When you select Apply to all processes with selected name, the action applies to all of the processes with the same name, even if they are not on the same page. That is, if you have 80 processes that are named **Process1**, but only 20 are visible, Guardium marks all 80 processes as either read or signed.

4. Click Search. The page refreshes with the search results.

5. The options for viewing the To Do items are as follows:

- View: Click to open a dialog to view details about the process, including distribution status and comments. In this dialog, you can
  - Sign Results: The receiver must have Sign Off enabled to be allowed to sign off.
  - Escalate: Add a Receiver to Review or Review and Sign.
  - Comment: View and add comments.
  - Download PDF: downloads a PDF of the process to your local drive.
  - PDF options: Recreate PDF, and Report (the current results), Diff (difference between one earlier report and a new report), or Reports and Diff (both). Note: The selection of PDF Content applies to both PDF attachments and PDF export files. Diff is available only after the first time this task runs since Diff requires a previous result. The maximum number of rows that can be compared at one time is 5000. If the number of result rows exceeds the maximum, the message compare first 5000 rows only shows up in the diff result.
  - Other results for this process list: Click to view the timestamps of additional results for this process. Click  to open another report in a new window.
  - Compare with other results: compare results from different runs of the same process.
- Download as PDF: downloads a PDF of the process to your local drive.

6. Click Refresh to refresh the display.

Note: To send files to an external server without sending email and without adding results to the to-do list, define an audit process without receivers. In the Send results section, create a receiver, clear Add to to-do list in the New Receiver page and then delete all receivers (including the one you created). The results of the audit process are now available in the audit process builder and a user that has access to the audit process builder and the audit process can view the results in Guardium.

## To-Do Lists and Data Level Security

---

Use the View To-Do List of menu to see the to-do lists of other users. Unlike the menu of users with admin role, the menu for other users includes only those users who are under the current user in the Data Level Security (DLS) hierarchy. If you have the admin or exempt role, then all users are shown in the menu.

If you access another user's results, the data that is presented in the report is filtered according to the Data Level Security and the role of the selected user. For example, for a custom workflow, the data is filtered according to the role of the selected user and the status that is defined for their role.

If you have an admin role, you can view the results of a user in your hierarchy based on the Data Level Security and the role of the selected user. If you access the result for a user who is not under the hierarchy, then it shows the result by using the Data Level Security of the administrator and shows for all roles.

When a result is added to a user's to-do list because of a change in an event status, if the result is not already in the to-do list, then Guardium sends an email to the user. The email does not contain a PDF, just a notification and link.

If a user goes to some other user's to-do list, a message indicates which user is determining the DLS filtering.

## Comparing discovery and classification results

---

Compare results from different runs of the same discovery and classification process.

### Procedure

---

1. Open the audit process to-do list and click View to open the results of a classification process.  
For more information, see [Audit Process To-Do List](#).
2. From the results window, click Compare with other results to open the results-comparison dialog.
3. From the results-comparison dialog, select the timestamp of another set of results from the same process and click Go to open the Classification run results compare view window.
4. Work with the information presented in the results-comparison view:
  - a. Use the Compare results menu to change the timestamp of the process results being compared.  
The results selected here are compared to the results of the process selected in step 1.  
Note: The results being compared are listed by timestamps in the Later results and Earlier results fields of the results-comparison view.
  - b. Use the View menu to define what is shown in the comparison view.  
The View menu includes the following options:
    - Rows unique to the later results displays only rows unique to the newer results.
    - Rows unique to the earlier results displays only rows unique to the earlier results.
    - Unchanged rows displays only rows that are unchanged between both sets of results.

Each option indicates the number of included rows, for example Rows unique to the later results (27) indicates that there are 27 rows unique to the later results.

## Related concepts

---

- [Audit Process To-Do List](#)

## Related reference

---

- [modify\\_guard\\_param](#)

# Using the host references report

The Host references report provides an easy way to identify where a server is used in Guardium and simplifies the process of decommissioning that server or updating its host name or IP address.

## About this task

---

The report returns all instances of a host name or IP address from the following Guardium locations:

- Custom tables
- Datasources
- Datasource groups
- Discover sensitive data scenarios (classification processes)
- Groups
- Policy rules
- Queries
- Security assessments

Note: Querying a host name returns instances of that host name or its associated IP address. Querying an IP address returns instances of that IP address or its associated host name.

Run the report from any Guardium system by using the Audit Process Builder. In a centrally managed environment, running the report on the central manager provides the best performance.

The following procedure describes running the report on an ad hoc basis by generating a one-time report of where an IP address is used. For more information about building and scheduling audit process, see [Building audit processes](#).

## Procedure

---

1. Go to Comply > Tools and Views > Audit Process Builder.
2. Create an audit process by clicking the  icon.
3. In the Name and archive panel, use the Name field to name the audit process. Click Next to continue.
4. In the Add tasks panel of the audit process builder, click the  icon to create a new task.  
Complete the following steps by using the New Task dialog.
  - a. Set the Task type to Report.
  - b. Use the Name field to name the task.
  - c. Set the Report field to Host references.
  - d. In the Task parameters section, use the Host name or IP address field to specify the host name or IP address of a server in your Guardium environment.
  - e. Click OK to close the dialog and save the task.
5. To immediately run the report and see the results, open the Run audit process panel and click Run Once Now.  
For information about defining a complete audit process with receivers and a schedule, see [Building audit processes](#).
6. View the results by clicking View Results.

# Audit and Report

Guardium organizes the data it collects into a set of domains. Each domain contains a different type of information relating to a specific area of concern: data access, exceptions, policy violations, and so forth.

All domains and their entities are described in [Domains, Entities, and Attributes](#).

Access to each domain within the Query-Report Builder is controlled by security roles. For detailed instructions on how to build queries, see [Using the Query-Report Builder](#).

In addition to the standard set of domains, users can define custom domains to contain information that is uploaded to the Guardium appliance. For example, your company might have a table relating generic database user names (hr23455 or qa4872, for example) to real persons (Paula Smith, John Doe). Once that table has been uploaded, the real names can be displayed on Guardium reports, from the custom domain. For more detailed information on how to define and use custom domains, see [External data correlation](#).

# External data correlation

This topic describes creating and managing custom tables and custom domains, for importing enterprise information to use with existing Guardium internal data.

You might have valuable information in various databases in your environment. It can be useful for an audit report to correlate relevant information from your databases with the data that is collected by Guardium. You can create custom tables on Guardium that combine enterprise information with existing Guardium internal data. You can then create queries for this information as if it were predefined data.

For example, you have a table that contains all employees, their database usernames, and the department to which they belong (such as, Development, Financial, Marketing, or HR). You can upload this table and all its data, and cross-reference this table with Guardium's internal tables. You can then see, for example, which employees from Marketing are accessing the financial database (which might constitute a suspicious activity).

For more information about data marts, see [Data Mart](#).

## Custom tables

Browse to the Custom Table Builder by using one of the following paths:

- Comply > Custom Reporting > Custom Table Builder
- Reports > Report Configuration Tools > Custom Table Builder

A custom table contains one or more attributes that you want to have available on the appliance. By uploading data for that table from an existing table, you can relate the encoded and real names.

Before you define a custom table, verify that the data you need from the existing database is a supported data type. A data type is supported if it is taken as one of the following SQL type by the underlying JDBC driver: INTEGER, BIGINT, SMALLINT, TINYINT, BIT, BOOLEAN, DECIMAL, DOUBLE, FLOAT, NUMERIC, REAL, CHAR, VARCHAR, DATE, TIME, TIMESTAMP. The following table summarizes some of the supported and unsupported data types for uploading to a custom table.

**Enterprise reports with custom tables:** If for any reason, the central manager did not receive data from a managed unit for the custom table in an enterprise report in the last 24 hours, the Guardium® UI banner displays the message:

Central manager experienced failure getting data from collector. Central manager experienced error in the last 24 hours uploading data.

Click the report name to open the Scheduled Jobs Exceptions report and view details of the managed units that had exceptions.

## Supported and unsupported data types for custom tables

Use this table to see the supported and unsupported data types for certain databases.

Table 1. Supported and Unsupported Data Types for Custom Tables

| Databases | Supported Data Types                                                                                                                             | Unsupported Data Types                                                          |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| Oracle    | float number char varchar2 date nchar nvarchar2                                                                                                  | long clob raw nclob longraw bfile rowid urowid blob                             |
| DB2®      | char varchar bigint integer smallint real double decimal date time timestamp                                                                     | blob blob longvarchar datalink                                                  |
| Sybase    | char nchar varchar nvarchar int smallint tinyint datetime smalldatetime                                                                          | text binary varbinary image timestamp                                           |
| MS SQL    | bigint bit char datetime decimal float int money nchar numeric nvarchar real smalldatetime smallint tinyint smallmoney varchar unique identifier | text                                                                            |
| Informix® | char nchar integer smallint decimal smallfloat float serial date money varchar nvarchar datetime                                                 | text                                                                            |
| MySQL     | bigint decimal int mediumint smallint tinyint double float date datetime timestamp time year<br>char binary enum set                             | longtext tinyblob tinytext blob text mediumblob<br>mediumtext longblob longtext |

Note: Blob value (even a value of 1 K) in dynamic SQL can be captured, but same size blob value in static SQL cannot be captured.

## Archiving and restoring custom tables

From the Custom Table Builder, select a table to manage and then select Purge/Archive to open the Custom Table Data Purge page.

Click Archive to include the data in the custom table in the normal data archive. The selected custom table data is archived according to the date in SQLGUARD\_TIMESTAMP column of the custom table.

You can archive data from either a collector or an aggregator.

When you prepare archived data to restore, keep in mind the following points:

- You can restore data to any collector or aggregator that is managed by the same central manager as the source collector. The metadata must be available or the custom table data cannot be restored.
- Data that is archived from an aggregator can be restored to any aggregator managed by the same central manager as the source aggregator.
- If the custom table structure changes between the archive time and the restore time in a way that results in an SQL error (for example, columns are removed or the type changes), then a warning message appears on the aggregation/archive activity report and the data is not restored.
- If a custom table is included in the default purge, then the restored data is kept for the number of days that are specified on the restore screen.
- If the custom table is set to overwrite data when it uploads, then restored data is deleted when the upload occurs.

## Custom domains

A custom domain contains one or more custom tables. If it contains multiple tables, you define the relationships between tables when you define the custom domain.

## Custom queries

A custom query accesses data from a custom domain. Use the Custom Query Builder to create queries against custom domains. Custom queries can then be used like any other query to generate reports or audit tasks, populate groups, or to define aliases.

## Database entitlement reports

DB Entitlement Reports use the Custom Domain feature to create links between the external data on the selected database with the internal data of the predefined entitlement reports. See topic, [Link External Data to Internal Data](#), on this subject. For more information about using predefined database entitlement reports, see [Running database entitlement reports](#). To see entitlement reports, log on to the user portal, and go to the DB Entitlements tab.

## LDAP import into custom tables

Enrich Guardium tables with LDAP data by using an LDAP server as a datasource. Retrieve and configure LDAP attributes that can be used to customize reports.

1. Open the Custom Table Builder.
2. To create a new table definition, click Manually Define and define the entity. For more information, see [Manually defining a table definition](#).
3. From the Custom Table Builder screen, select your custom table definition and click LDAP Import.
4. Click  to create a new LDAP datasource.
  - From the Configuration tab, specify the LDAP connection information and define the Base DN. The Base distinguished name (DN) specifies the starting point of the search in the LDAP tree. Optionally include a search filter in LDAP search syntax. For example, `objectClass=person`.
  - Click the Mapping tab to map the columns of the custom table to the LDAP fields.
  - Click the Schedule tab and add a schedule to import the LDAP data.
  - Click Save to save the configuration.
5. To import data, select the LDAP Host from the LDAP configurations screen and click Run Once Now or wait for the schedule that you defined.  
Tip: To view the imported LDAP data, click the LDAP datasource from the Custom Tables list, and click Edit Data.

The custom table now has LDAP data that can be used to create custom reports.

You can configure custom tables for LDAP in the Guardium CLI by using the following GuardAPI commands:

- [Create custom table for LDAP import](#)
- [Update custom table for LDAP import](#)
- [Delete custom table for LDAP import](#)
- [List custom table for LDAP import](#)
- [Run custom table for LDAP import](#)

To import an existing table structure, see [Uploading a table definition](#).

## Uploading a table definition

Create a custom table by the uploading a table definition. You can access the table's metadata from the database server on which the metadata is defined.

Note: Custom Tables uploaded to Guardium are optional components enabled by product key. If these components are not enabled, the Custom Tables choices listed do not display in the Custom Table Builder selection.

1. From the Custom Table Builder, click Upload Definition to open the Import Table Structure page. It is not necessary to select an item.
2. Enter a description for the table in the Entity desc field. This is the name you use to reference the table when you create a custom query.
3. Enter the database table name for the table in the Table Name field. This is the name you use to create the table in the local database.
4. Enter a valid SQL statement for the table in the SQL Statement field. The result set returned by the SQL statement must have the same structure as the custom table that you define. For example, if the custom table contains all columns from the table named `my_table`, enter `select * from my_table`.  
Note: Do not include any newline characters in the SQL statement. All columns must be explicitly named; if needed, use a column alias.
5. Click Add Datasource to open the Select datasource window. From Select datasource, you can define where the external database is located, and the credentials that are needed to retrieve the table definition and content later in the process.
6. Use Select datasource to identify the database from where you will upload the table definition.
7. Click Retrieve to upload the table definition. The SQL statement runs and retrieves the table structure. The SQL request is sent to the external database from the Guardium system. Remember that only the definition is being uploaded. You can upload data later.

## Manually defining a table definition

1. From the Custom Table Builder, click Manually Define to open the Define Entity panel.
2. Enter a description for the table in the Entity desc field. This is the name you will use to reference the table when creating a custom query. Use of the special characters `\$|&;`"` are not allowed in the entity description.
3. Enter the database table name for the table in the Table Name field. This is the name you will use to create the table in the local database.
4. For each column in the table to be defined:
  - Enter a name in the Column Name box. This will be the name of the column in the database table.
  - Enter a name in the Display Name box. This is the name you will use to reference the attribute in the Custom Domain Builder and the Custom Query Builder.
  - Select a data type (Text, Date, Integer, Float, or TimeStamp).
  - For a Text attribute, enter the maximum number of characters in the Size box. (The Size box is not available for other data types.)
  - If uniqueness is to be enforced on the column, check the Unique box.
  - If the attribute being defined corresponds to a group type, select that group type from the Group Type list.
  - Click Add to add the column.
5. Use the Entity Key drop-down list to identify which column will be used as the entity key. The Entity Key is used in the query builder when selecting count.
6. If additional changes are made after the Add button, such as deletion of a column, or changing an attribute, Click Apply to save any changes.
7. Click Done when you have added all columns for the table.

## Modifying a table definition

If you modify the definition of a custom table, you may invalidate existing reports based on queries using that table. For example, an existing query might reference an attribute that has been deleted, or whose data type has been changed. When applying changes to a custom table, if any queries have been built using attributes from that table, the Queries are displayed in the Query List panel. Note: You can also use the Modify to view and validate the table structures that were imported.

1. From the Custom Table Builder, select the custom table to modify.
2. Click Modify to open the Modify Entity page.
3. For information about modifying a table definition, see [Manually defining a table definition](#).

4. After you apply changes to a custom table, if any queries might be invalid due to changes to attributes from that table, the queries are displayed in the Query List page. Use Query List to choose and change queries. You do not have to make all changes immediately as you can always come back and use the Check for Invalid Queries option.

## Invalid queries

---

If you modify the definition of a custom table, you may invalidate existing reports based on queries using that table. For example, an existing query might reference an attribute that has been deleted, or whose data type has been changed. It is a good idea to check for invalid queries after the table modification process.

1. From the Custom Table Builder, click Invalid Queries.
2. The queries are displayed in the Query List panel. Use Query List to choose and change queries.

## Purging data from a custom table

---

Data can be purged from custom tables on the Guardium server on demand, or on a scheduled basis.

1. From the Custom Table Builder, select a custom table to purge.
2. Click Purge to open the Custom Table Data Purge panel.
3. Click Purge All to purge now.

Note: Run once now purge will look at the RESTORED\_DATA table for retention. Purge ALL will purge all records that are deleted without checking the retention.

4. In the Configuration panel, enter the age of the data to be purged, as a number of days, weeks or months prior to the purge operation date.
5. Click Run Once Now to run a schedule purge operation once.
6. Click Modify Schedule to open the standard Schedule Definition panel and schedule a purge operation.
7. Click Done to close the panel.

## Uploading data to a custom table

---

1. From the Custom Table Builder, click on the name of the table whose data you want to upload.
2. Click Upload Data to open the Upload Data page.
3. In the SQL statement box, enter a valid SQL statement for the table. The result set returned by the SQL statement must have the same structure as the custom table defined. For example, if the custom table contains all columns from the table named my\_table, enter `select * from my_table`.

Important: Different SQL databases have unique syntax requirements. For example, compare the following SQL statements for uploading from an Oracle database and uploading from a Microsoft SQL Server database:

```
Oracle example
select * from xxx WHERE coll > TO_DATE('^FromDate^', 'YYYY/MM/DD HH24:MI:SS');

#Microsoft SQL Server example
select * from xxx WHERE coll > CONVERT(DATETIME, '^FromDate^');
```

To create a functional SQL statement for uploading data, test the statement outside of Guardium with the SQL interface of the specific database being used.

Do not include any newline characters in the SQL statement.

The following fields, which are internal to Guardium, are available for use within SQL statements:

- `^FromDate^` and `^ToDate^` where the value is equal to the previous upload date and the current upload date, respectively.
- `^fromID^` where the value is equal to the maximum value of the ID column from the previous upload.

Important:

- When you use `^FromDate^` or `^ToDate^` do not specify an Id column name.
- When you use `^fromID^`, specify an Id Column name and Id column type.

4. If using `^fromID^` specify the ID column name and Id column type for the table defined within the datasource. The specified column name is used for tracking by ID.
5. In the DML command after upload box, enter a DML command (an update or delete SQL statement) with no semicolon, to be executed after uploading the data.

Note: Do not include any newline characters in the SQL statement.

6. To configure Overwrite Default Purge, select Per upload to purge data in the custom table before the upload. Select Per datasource to purge data for that datasource before the upload.

7. Check Default Purge (in the Upload Custom Data screen) to be part of the Default Custom Table Purge Job purge object which has an initial default age of 60 days.

To add a purge schedule for this table, go to initial Custom Table Builder page, select a custom table and click Purge to open a Custom Table Data Purge configuration screen.

8. Check the Use default schedule box only if uploading tables from previous versions of Guardium. This check box only appears in a central manager view and only for the following predefined custom tables: CM Buffer Usage Monitor, Enterprise No Traffic, S-TAP Changes, and S-TAP Info.

9. Click Add Datasource to open the Select Datasource page. From Select Datasource you can identify one or more databases from which to upload the table data. You can add multiple datasources to upload from multiple sources.

Notes:

- For a central manager, on the Import Data page, you can select Include default source. If this box is checked, upload data iterates through all online registered managed units.
- When adding a datasource, the application cannot be scheduled to run without specifying the user name and password of the selected datasource.

10. You can click Check/Repair to compare the schema of the custom table to the schema of the meta-data. In a central management environment, the custom table definition resides on the central manager, and the custom table may not exist on the local (managed unit) database. Click the Check/Repair button to check if the custom table exists locally, and create one if it does not.

11. Click Verify Datasources to test the external database connection. An acknowledgment screen will appear.

12. Click Apply.

13. To upload data to this custom table, do one of the following:

- Click Run Once Now to upload data manually.
- Check Modify schedule to configure the schedule.

## Maintaining custom tables

---

When following the procedure for creating a Custom Table (detailed previously) and selecting a predefined custom table, click Maintenance to manage the table engine type and table index. The table engine types for custom tables/entitlements (InnoDB and MyISAM) will appear for all predefined custom databases as the data stored on the Guardium internal database is MySQL-based. The two major types of table storage engines for MySQL databases are InnoDB and MyISAM. Major differences between these MySQL table engine types:

- InnoDB is more complex while MyISAM is simpler.
- InnoDB is more strict in data integrity while MyISAM is looser.
- InnoDB implements row-level lock for inserting and updating while MyISAM implements table-level lock.
- InnoDB has transactions while MyISAM does not.
- InnoDB has foreign keys and relationship constraints while MyISAM does not.

Note:

- Changing the engine type is disallowed (and the selection grayed out) if the row number in the table is greater than 1M.
- The Length for Text Columns field does not apply to and is not saved for integer-only columns.

The other selection in the Maintain Custom Table menu is Manage Table Index. Click Insert to open Table Index Definition. The pop-up screen suggests columns in the table to add to indexes based on columns used on custom domains as Join conditions. Select the columns and save. Indexes will be created (or re-created).

To maintain performance, MySQL allows a maximum length for indexes:

- MyISAM : 1000 bytes = 333 characters
- InnoDB: 3072 bytes = 1024 characters

The utf8mb3 character set uses 3 bytes per character. If columns with more characters than the limit are required, use a subset of the column length.

For example, instead of :

```
create index a1 on CUSTOM.aaa (id, `System` (255), aaa(255), qqq(255));
```

Use:

```
create index a1 on CUSTOM.aaa (id, `System` (100), aaa(100), qqq(100));
```

## Scheduling custom data uploads

Once a custom table definition is in place, data can be uploaded to custom tables on the Guardium appliance on a scheduled basis.

Note: New installations do not automatically start Enterprise reports. There is one upload schedule for each custom table. The total amount of disk space reserved on the Guardium appliance for custom tables is 4GB.

1. Open the Custom Table Builder.
2. Choose a custom table by clicking on the entity label and highlighting it.
3. Click Upload Data to open the Import Data panel.
4. Mark the Use Default Schedule check box to upload this table using the default schedule. Otherwise, this custom table uses its own upload data schedule.
5. Click Modify Schedule to open the standard Schedule Definition panel and modify the schedule.
6. Click Done when you are finished.

The Enterprise reports custom upload are like other jobs. There are two ways to enable them:

- In the Custom Table Upload GUI. (requires license for custom upload)
- Use GuardAPI from the CLI:

```
grdapapi add_schedule jobName=CustomTablePurgeJob_CM_SNIFTER_BUFFER_USAGE obGroup=customTableJobGroup Enterprise S-TAPS
Changed: grdapapi add_schedule jobName=customTableDataUpload_106 jobGroup=customTableJobGroup CM Buffer Usage Monitor:
grdapapi add_schedule jobName=customTableDataUpload_104 jobGroup=customTableJobGroup S-TAP Info: grdapapi add_schedule
jobName=customTableDataUpload_80 jobGroup=customTableJobGroup
```

Attention: When scheduling custom table jobs, the Start Time defines the time at which the schedule begins each day. For example, setting Start Time to 4 p.m. means the schedule will run from 4 PM until midnight each day. To create schedules that run continuously throughout the day, set Start Time to 12 a.m. (Midnight).

## Creating a custom domain

After defining one or more custom tables, define a custom domain so that you can perform query and reporting tasks using the custom data. The information collected is organized into domains, each of which contains a different type of information relating to a specific area of concern: data access, exceptions, policy violations, etc. There is a separate query builder tool for each domain. Custom domains allow for user-defined domains and can define any tables of data uploaded to the Guardium appliance. See [Custom Domains](#). The usage for these custom entitlement (privileges) domains are for entitlement reports which are found if logged in as a user. To see these reports, go to the user tab, DB Entitlements.

Note: DB Entitlements Domains are optional components enabled by product key. If these components have not been enabled, the choices listed in the Custom Domains help topic will not appear in the Custom Domain Builder selection.

1. Open the Custom Domain Builder by navigating to one of the following:
  - Comply > Custom Reporting > Custom Domain Builder
  - Reports > Report Configuration Tools > Custom Domain Builder
  - Comply > Custom Reporting > Custom Domain Builder
2. Click Domains to open the Domain Finder panel.
3. Click New to open the Custom Tables Domain panel.
4. Enter a Domain Name. Typically, you will be including a single custom table in the domain, so you may want to use the same name for the domain.
5. The Available Entities box lists all custom tables that have been defined (and to which you have access). Select an entity. Optionally, click the (Filter) tool to open the Entity Filter and enter a Like value to select only the entities you want listed, and click Accept. This closes the filter window and returns you to the Custom Tables Domain panel, with only those entities matching the Like value listed in the Available Entities box. Select the entity you want to include.
6. Click the >> arrow button to move the entity selected in the Available Entities list to the Domain Entities list.
7. To add an entity to a domain that already has one or more tables, follow these steps. You will need to use the Join Condition to define the relationship between the entities. For each additional entity:

- Note: When data level security is on, internal entities added to the custom domain cannot belong to different domains with filtering policies.
- a. From the Domain Entities box, select an entity. All of the attributes of that entity will become available in the field drop-down list of the Domain Entities box. Select the attribute from that list that will be used in the join operation.
  - b. From the Available Entities list, select the entity you want to add. All of the attributes of that entity will become available in the field dropdown list of the Available Entities box. Select the attribute from that list that will be used in the join operation.
  - c. Select = (the equality operator) if you want the join condition to be equal (e.g., domainA.attributeB = domainC.attributeD). Select outer join if you want the join condition to be an outer join using the selected attributes.
- Note: Known limitation: After an entity is added, the Detail window in the GUI always displays it as an inner join. However, the correct join condition is saved in the table.
- d. Click Add Field Pair. Add Field Pair can be used to add more attributes pairs of these two entities to the join condition.
  - e. Repeat the steps for any additional join operations.
8. Select the Timestamp attribute for the custom domain entity.
- Note: At least one entity with a timestamp must be used, since a timestamp is required to save a custom domain.
9. Click Apply.

## Modifying a custom domain

---

The goal is to create a linkage between external data and the internal data.

1. Open the Custom Domain Builder.
2. Choose the Custom Domain that you wish to clone.
3. Click Modify to open the Custom Tables Domain panel.
4. See Open Custom Domain Builder and Linking External Data to Internal Data for assistance.
5. Click Apply to save the changes.

## Removing a custom domain

---

1. Open the Custom Domain Builder.
2. Choose the Custom Domain that you wish to clone.
3. Click Domains to open the Domain Finder panel.
4. Click Delete to remove the custom domain.

## Cloning a custom domain

---

1. Open the Custom Domain Builder.
2. Choose the Custom Table that is in the domain you wish to clone.
3. Click Domains to open the Domain Finder panel.
4. Click Clone to open the Custom Tables Domain panel.
5. Change the Domain Name to reflect the new domain.
6. See Open Custom Domain Builder and Linking External Data to Internal Data for assistance.
7. Click Apply to save the changes.

## Linking external data to internal data

---

The goal is to create a linkage between external data and the internal data.

1. Open the Custom Domain Builder.
2. Choose the Custom Table that has your external data.
3. Click Domains to open the Domain Finder panel.
4. Click Modify to open the Custom Tables Domain panel.
5. Click the Filter icon next to the Available Entities.
6. Un-check the Custom box for the filter and optionally fill in a Like condition to filter entity names and click Accept.
7. Select an entity from the Available Entities that you would like to link with your external data.
8. Select the field that will be used to join data with your external data.
9. Highlight the table from the Domain Entities that contains your external data
10. Select the field that will be used to join data with the internal data.
11. Click the Add Field Pair to add the relationship.
12. Click the double arrow >> to add the internal table to the Domain Entities list.
13. Click Apply to save the changes.

## Working with custom queries

---

This section describes how to open the Custom Query-Report Builder. For more information about defining a query, see [Using the Query-Report Builder](#). Use the Custom Query Builder to build queries against data from custom domains, which contain one or more custom tables.

1. From the Custom Query Builder, select a custom domain from the list. The list of queries/reports under this domain opens.
2. To view, modify or clone an existing query, select it from the Query Name list.

## Bidirectional interface to and from InfoSphere Discovery

---

Both IBM® Guardium and InfoSphere® Discovery can identify and classify sensitive data, such as social security numbers or credit card numbers.

A Guardium customer can use a bidirectional interface to transfer identified sensitive data information from one product to another. Those customers who have already invested the time in one InfoSphere product can transfer the information to the other InfoSphere product.

Note: In Guardium, the Classification process is an ongoing process that runs periodically. In InfoSphere Discovery, Classification is part of the Discovery process that usually runs once.

The data is transferred via CSV files.

The summary of Export/Import procedures is as follows:

- Export from Guardium - Run the predefined report (Export Sensitive Data to Discovery) and export as CSV file.
- Import to Guardium - Load to a custom table against CSV datasource; define default report against this datasource.

Follow these steps:

- Export from Guardium
  - Export Classification Data from Guardium to InfoSphere Discovery
1. As an admin user in the Guardium application, go to Tools > Report Building > Classifier Results Tracking > Select a Report > Export Sensitive Data to Discovery.  
Note: Add this report to the UI pane (it is not by default).
  2. Click the Customize icon on the Report Result screen and specify the search criteria to filter the classification results data to transfer to Discovery.
  3. Run the report and click Download All Records.
  4. Save as CSV and import this file to Discovery according to the InfoSphere Discovery instructions.

Import to Guardium

Import Classification Data from InfoSphere Discovery to IBM Guardium

1. Export the classification data as CSV from InfoSphere Discovery based on InfoSphere Discovery instructions.
2. Open the Custom Table Builder by navigating to either of the following:
  - Comply > Custom Reporting > Custom Table Builder
  - Reports > Report Configuration Tools > Custom Table Builder
3. Select ClassificationDataImport and click Upload Data.
4. In Upload Data screen, click Add Datasource, click New, define the CSV file imported from Discovery as new datasource (Database Type = Text).  
Note: Alternatively you can load the data directly from Discovery database if you know how to access the Discovery database and Classification results data.
5. After defining the CSV as Datasource, click Add in Datasource list screen.
6. In Upload data screen click Verify Datasource and then Apply.
7. Click Run Once Now to load the data from the CSV.
8. Go to Report Builder, select the Classification Data Import report, Click Add to Pane to add it to your Portal and then navigate to the report.
9. Access the Report, click Customize to set the From/To dates and execute the report.

The report result has the classification data imported from InfoSphere Discovery. Double-click to invoke APIs assigned to this report. The data imported from Discovery can be used for the following:

- Add new Datasource based on the result set.
- Add/Update Sensitive Data Group.
- Add policy rules based on datasource and sensitive data details.
- Add Privacy Set.

## CSV interface signature

The following table provides examples of CSV interface signatures used in the bidirectional transfer between Guardium and InfoSphere Discovery.

Table 2. CSV Interface signature

| Interface signature                                        | Example                                              |
|------------------------------------------------------------|------------------------------------------------------|
| Type                                                       | Db2                                                  |
| Host                                                       | 9.148.99.99                                          |
| Port                                                       | 50001                                                |
| dbName (Schema name for Db2 or Oracle, db name for others) | cis_schema                                           |
| Datasource URL                                             |                                                      |
| TableName                                                  | MK_SCHED                                             |
| ColumnName                                                 | ID_PIN                                               |
| ClassificationName                                         | SSN                                                  |
| RuleDescription                                            | Out-of-box algorithm of InfoSphere Discovery         |
| HitRate                                                    | 70% - not available for export in Guardium Vers. 8.2 |
| ThresholdUsed                                              | 60% - not available for export in Guardium Vers. 8.2 |

## Privacy sets

A privacy set is a collection of elements that can be used to do special monitoring.

A privacy set consists of one or more object-field pairs - for example, the salary field of the employee table, or all fields of the salary history table. All access to these elements within a given time frame can be reported.

Select any of the topics to work with privacy sets.

## Open the privacy set builder

To access a privacy set definition, your Guardium® user account must be assigned a security role that is also assigned to that privacy set definition. Privacy sets that you cannot access will not display in a list of privacy sets.

To open the Identify Privacy Set page, browse to one of the following locations:

- Comply > Tools and Views > Privacy Set Builder
- Discover > Database Discovery > Privacy Set Builder

From the Identify Privacy Set you can create a new privacy set, modify an existing privacy set, or run a privacy set report.

## Creating a privacy set

---

1. Click the  icon to open the Privacy Set Definition page.
2. In the Privacy Set Description box, enter a unique name for the privacy set. Do not include apostrophe characters in the name. This is the name that will display in the Identify Privacy Set panel.
3. From the Security Classification drop-down list, optionally select a security classification for this privacy set.
4. In the Elements in this Privacy Set pane, for each element pair to include:
  - Enter an object name in the Object box.
  - Enter a field name in the Field box, or mark the Any Field in this Object box to include all fields contained in the specified object.
  - Click Add this new Object – Field Pair.
5. When all elements have been added, click Save.
6. Optionally, click the Roles button to add Roles.
7. Optionally, click the Comments button to add comments.

## Modifying a privacy set

---

1. Select the privacy set you want to modify and click Modify.
2. Make the changes you want to the privacy set definition.
3. Click Save.
4. Click Done when you are finished.

## Cloning a privacy set

---

1. Select the privacy set you want to clone and click Clone.
2. The cloned privacy set is named COPY OF selected privacy set. Guardium suggests that you change this name to something more meaningful.
3. Make any additional changes to the privacy set definition, as necessary. F
4. Click Save.
5. Click Done when you are finished.

## Deleting a privacy set

---

If an auditing process is running, you cannot remove a privacy set. Stop the auditing process, then follow the steps to remove the privacy set.

1. Select the privacy set you want to delete.
2. Click Delete and confirm the action.
3. Click Done.

## Running a privacy set report

---

This procedure describes how to run a privacy set report on demand. To schedule a privacy set report, include it in a compliance workflow (see Compliance Workflow Automation).

1. Select a privacy set from the privacy set list and click Run.
2. In the Task Parameters, enter the starting and ending times for the task.
3. Specify how to display the results:
  - Report by Access Details - Default. Displays the access count for each combination of client IP, server IP, server (name), server type, database protocol, source program name, and database user name
  - Report by Application User - Displays a separate column with that name (following DB User Name) and the output is additionally qualified by the application user.
4. Click Run Once Now. After the report has been executed, it will be displayed in a separate window.
5. Click Done.

---

## Custom Alerting

Alert messages can be distributed via e-mail, SNMP, syslog, or user-written Java™ classes. The last option is referred to as custom alerting.

When an alert is triggered, a custom alerting class can take any action appropriate for the situation; for example, it might update a Web page or send a text message to a telephone number.

To create a custom alerting class, first contact Technical Support to obtain the necessary interface file. The following topic describes how to implement the interface. See Use the Custom Alerting Interface, and also the following topic which contains an example: Sample Custom Alerting Class.

Once the class has been compiled, it must be uploaded to the Guardium® appliance. See Manage Custom Classes.

For guidelines on testing a custom alerting class, see the Test a Custom Alerting Class section later in this topic.

Note: Do not take or run custom code from untrusted data sources to order to reduce the risk of security vulnerabilities.

Note: Do not take or run custom code from untrusted sources.

Note: Do not write a custom class that gets data from an untrusted source.

---

## Use the Custom Alerting Interface

The custom alerting class must be in the com.guardium.custom package and must implement the com.guardium.custom.alerts.CustomerDefinedAlertingIfc interface:

```
package com.guardium.custom
public class YourClassNameHere implements CustomerDefinedAlertingIfc {
```

The interface contains the five methods described.

Table 1. processAlert Method

| Method 1    |                                                                                                                         |
|-------------|-------------------------------------------------------------------------------------------------------------------------|
| Description | Process a single alert message.                                                                                         |
| Syntax      | public void processAlert (String message, Date timeStamp)                                                               |
| Parameters  | A String containing the message generated by the alert.<br>A java.util.Date for the time the alert message was created. |

Table 2. getMessage Method

| Method 2    |                                        |
|-------------|----------------------------------------|
| Description | Return the alert message               |
| Syntax      | public String getMessage ()            |
| Parameters  | A String containing the alert message. |

Table 3. getTimeStamp Method

| Method 3    |                                                              |
|-------------|--------------------------------------------------------------|
| Description | Return the timestamp associated with the alert message.      |
| Syntax      | public Date getTimeStamp ()                                  |
| Parameters  | A java.util.Date for the time the alert message was created. |

Table 4. setMessage Method

| Method 4    |                                           |
|-------------|-------------------------------------------|
| Description | Set the alert message.                    |
| Syntax      | public void setMessage (String inMessage) |
| Parameters  | A String containing the alert message.    |

Table 5. setTimeStamp Method

| Method 5    |                                                              |
|-------------|--------------------------------------------------------------|
| Description | Set the timestamp associated with the alert message.         |
| Syntax      | public void setTimeStamp (Date inDate)                       |
| Parameters  | A java.util.Date for the time the alert message was created. |

## Sample Custom Alerting Class

The following sample program implements the five methods described in the previous section. For the processAlert method, this program simply writes the alert message and timestamp to the system console.

```
/*
 * Sample Custom Alerting Class
 *
 */
package com.guardium.custom;
import java.text.DateFormat;
import java.util.Date;
public class HandleAlerts implements CustomerDefinedAlertingIfc {
private String message = "";
private Date timeStamp = null;
public void processAlert(String message, Date timeStamp) {
setMessage(message);
setTimeStamp(timeStamp);
System.out.println(getMessage() + " on " +
DateFormat.getDateInstance().format(getTimeStamp()));
}
public void setMessage(String inMessage) {
message = inMessage;
}
public String getMessage(){
return message;
}
public void setTimeStamp(Date inDate){
timeStamp = inDate;
}
public Date getTimeStamp(){
return timeStamp;
}
}
```

## Test a Custom Alerting Class

After compiling a custom alerting class, follow the procedure to test it.

1. Upload the custom class to the appliance. This is an administration function that is performed from the Administrator Console. See Manage Custom Classes.
2. Define a correlation or real-time alert to use the custom alerting class. Regardless of which alert type generates the alert, testing is easier if you assign a second notification type (email, for example) against which you can compare the custom alerting results.
3. Check the environment by doing one of the following:
  - For a correlation alert:

- Check that the Anomaly Detection polling interval is suitable for testing purposes and that Anomaly Detection has been started. If the polling interval is too long (it may be 30 minutes or more), you may have a long wait before the query runs.
  - Check that the Alerter polling interval is suitable for testing purposes and that the Alerter has been started.
  - Check that the alert to be tested has been marked Active.
  - For a real-time alert:
    - Check that policy containing the rule with the custom alert action is the installed policy.
    - Verify that the inspection engine was restarted after the updated policy was installed.
    - Check that the Alerter polling interval is suitable for testing purposes and that it has been started.
4. Take whatever action is necessary to trigger the alert (generate a number of login failures, for example).
- 

## Flat Log Process

The Flat Log option is a process to allow the Guardium® appliance to log information without immediately parsing it in real time.

This saves processing resources, so that a heavier traffic volume can be handled. The parsing and amalgamation of that data to Guardium's internal database can be done later, either on a collector or an aggregator unit.

There are two Guardium features involving the Flat Log Process.

- Flat Log by throttling mechanism. This feature is implemented by running the CLI command, **store alp\_throttle 1**. The same policy that is applicable to real-time S-TAP traffic is used to process traffic that was logged by the flat log process. For Flat Log by throttling mechanism, do not select the Flat Log checkbox in the Policy Builder.
- Flat Log by policy definition. Selection of this feature involves **Setup > Tools and Views > Policy Installation and Manage > Activity Monitoring > Flat Log Process**.

Note: Rules on flat does not work with policy rules involving a field, an object, SQL verb (command), Object/Command Group, and Object/Field Group. In the Flat Log process, "flat" means that a syntax tree is not built. If there is no syntax tree, then the fields, objects and SQL verbs cannot be determined.

The following actions do not work with rules on flat policies: LOG FULL DETAILS; LOG FULL DETAILS PER SESSION; LOG FULL DETAILS VALUES; LOG FULL DETAILS VALUES PER SESSION; LOG MASKED DETAILS.

When the Log Flat (Flat Log) checkbox option listed in the Create New Policy pane of the Policy Builder is checked,

- Data is not parsed in real time.
  - The flat logs can be seen on a designated Flat Log List report.
1. Navigate to **Manage > Activity Monitoring > Flat Log Process**.
  2. Select the activity to perform:
    - Process - Merge the flat log information to the internal database.
    - Archive/Aggregation/Purge - Archive or aggregate, and optionally purge, the flat log.
    - Purge Only - Purge the flat log data.
  3. Click **Apply** to save the configuration.
  4. For a Process activity, do one of the following:
    - Click **Run Once Now** to merge the flat log information to the internal database immediately.
    - Click **Modify Schedule** to define a schedule for this activity. You can select the start time, restart frequency, and repeat frequency. For the **Schedule by..** field, you must select either Day/Week or Month. See [Scheduling](#) for more information about scheduling.

## Running database entitlement reports

Database entitlement reports provide up-to-date snapshots of database users and their required access privileges. Learn how to prepare and run these reports to validate and ensure that users have only the privileges that are needed to perform their duties.

### Before you begin

This task requires downloading scripts from a Guardium system and running those scripts on a database server. You need to identify the IP address of the machine that is used to access the Guardium system for downloading scripts. The address can be either an individual workstation where you download the scripts before you transfer them to a database server, or the database server itself. If the relevant scripts for Vulnerability Assessment are already download and run, you can start at step [5](#).

### About this task

Along with authenticating users and restricting role-based access privileges to data, even for the most privileged database users, periodically perform entitlement reviews: validate and ensure that users have only the privileges that are required to perform their duties. This process is known as database user rights attestation reporting.

You can use the Guardium predefined database entitlement (privilege) reports to see who has system privileges and who granted these privileges to other users and roles. Database entitlement reports are important for auditors who are tracking changes to database access, and to ensure that security holes do not exist from lingering accounts or ill-granted privileges.

DB entitlement reports use the Custom Domain feature of Guardium® to create links between the external data on the selected database with the internal data of the predefined entitlement reports. Predefined entitlement reports are available for many data sources, including: Oracle; MySQL; DB2®; Sybase; Sybase IQ; Informix®; MS SQL 2000/2005/2008; Netezza®; Teradata; and PostgreSQL; Db2 on z/OS. For MS SQL Server and Oracle databases you can also use [Entitlement Optimization](#) to access this information. For a full description of the domains in the DB entitlement reports, see [Database Entitlement Reports](#). (For more information about the Custom Domain Builder, Custom Query Builder, or Custom Table Builder, see [External data correlation](#).)

DB Entitlement Reports require access to the database and specific database privileges, similar to Vulnerability Assessments (VA). Both are enabled by scripts that are run in the database itself. (The scripts are used for both VA and entitlement reporting.) Use these database-specific SQL scripts as guidance to define database user roles that connect to the database. Once created, these groups or roles can be assigned to any database user who needs to run an assessment. The available scripts are:

- gdmonitor-db2.sql (for Db2)
- create\_CKADBVA\_schema\_tables\_zOS.sql (for Db2 on zOS)
- gdmonitor-db2-zOS.sql (for Db2 on zOS)
- gdmonitor-mss.sql (for MS-SQL 2005 and up)
- gdmonitor-mss.sql (for MS-SQL 2005 and up)
- gdmonitor-mss-SA.sql (for MS-SQL)
- gdmonitor-mys.sql (for MySQL)
- gdmonitor-netezza.sql (for Netezza)
- gdmonitor-ora.sql (for Oracle)
- gdmonitor-ora-container.sql (for Oracle Container DB)
- gdmonitor-postgres.sql (for PostgreSQL)
- gdmonitor-syb.sql (for Sybase)
- gdmonitor-teradata.sql (for Teradata)
- gdmonitor-sybaseIQ.sql (for SybaseIQ)
- Jconnect\_SybaseIQ\_requirement.txt (for SybaseIQ)
- gdmonitor-db2-IBMi.sql (for Db2 on iSeries)
- gdmonitor-Aster.sql (for Aster)
- gdmonitor-mongodb24.sql (for MongoDB 2.4)
- gdmonitor-mongodb26andAbove.sql (for MongoDB 2.6 and above)
- gdmonitor-hive-Cloudera.sql (for Hive on Cloudera Hadoop distribution)
- gdmonitor-Cloudera-Manager.sql (for Cloudera Manager)
- gdmonitor-DSE-Cassandra.sql (for DataStax Cassandra)
- gdmonitor-SAP-Hana.sql (For SAP Hana)
- gdmonitor-Apache-Cassandra.sql (For Apache Cassandra)
- gdmonitor-azure.sql (For SQL DB Azure)
- gdmonitor-Couchbase.sql (For Couchbase)
- gdmonitor-ifx.sql (For Informix)
- gdmonitor-mariaDB.sql (For MariaDB)
- gdmonitor-mongodb26-To-34.sql (For MongoDB version 2.6 to 3.4)
- gdmonitor-mongodb36andAbove.sql (For MongoDB version 3.6 and up)
- gdmonitor-mss2000-only.sql (For MS SQL Server 2000)
- gdmonitor-Neo4j.sql (For Neo4j)
- gdmonitor-ora-autonomous.sql (For Oracle autonomous)
- gdmonitor-ora-RDS.sql (For Oracle RDS)
- gdmonitor-PerconaMySQL.sql (For Percona MySQL)
- gdmonitor-postgres.sql (For PostgreSQL)
- gdmonitor-Redshift.sql (For Redshift)
- gdmonitor-Snowflake.sql (For Snowflake)
- gdmonitor-syb.sql (For Sybase)
- gdmonitor-sybaseIQ.sql (For SybaseIQ)
- gdmonitor-teradata.sql (For Teradata)

Important: Before you run any scripts, be sure to read the instructions in the script headers and review the database actions that the script takes.

## Procedure

---

1. On a Guardium system, enable the file server by using the **fileserver** CLI command.

For example, to enable the file server for 1 hour and download the scripts to a system with IP address **10.0.0.1**, use the following command:

```
fileserver 10.0.0.1 3600
```

When successfully initiated, the output is similar to:

```
Starting the file server...
The file server is ready at https://guardium.host.com:8445
The timeout has been set to 3600 seconds and it may timeout during the uploading.

The upload will only be accessible from the IP you are logged in from: 10.0.0.1

Press ENTER to stop the file server.
```

2. On the machine where you download the scripts, use a web browser to access the file server.

For example, to access the scripts on a Guardium system that runs at **https://guardium.host.com:8445**, enter the following URL:

```
https://guardium.host.com:8445/log/debug-logs/gdmonitor_scripts/
```

3. Download the required scripts using the web browser's Right-click->Save link as... action or a similar function.

Review the README.txt files to identify the correct scripts to use for specific database types.

4. Follow the instructions in the file header.

5. Add data sources or databases to the appliance.

6. Assign data sources to entitlements (browse to Comply->Custom Reporting->Custom Table Builder. Select the custom table listing of your entitlement. Click Upload Data. Assign data sources to the entitlement report at the Import Data menu screen. When you are done, click Run Once Now.

7. To see entitlement reports, type the report name in the Quick Search.
- 

## User Identification

Guardium® provides several methods to identify application users, when the actual database user is not apparent from the database traffic.

Some database applications are designed to use or share a small number of database user accounts. These applications manage their users independently of the database management system, which means that when observing database traffic from outside of the application, it can be difficult to determine the application user who is controlling a database connection at any given point in time. However, when questionable database activities occur, you need to relate specific actions to specific individuals, rather than to an account shared by groups of individuals. In other words, you must know the application user, not just the database user.

Guardium provides several methods to identify application users, when the actual database user is not apparent from the database traffic:

- Identify Users via Application User Translation - For some of the most popular commercial applications (Oracle EBS, PeopleSoft, SAP, etc.), Guardium can identify users automatically.
- Identify Users via API - The Application Events API allows you to signal Guardium when an application user takes or relinquishes control of a connection, or when any other event of interest occurs. (This can be used for more than just identifying users.)
- Identify Users via Stored Procedures - Many applications use database stored procedures to identify the application user. In these cases, user information can usually be extracted from the stored procedure parameters.

Within the enterprise, it may be necessary to employ several methods to identify users, depending on the applications used.

- **[Identify Users using the Application User Translation](#)**

Some applications manage a pool of database connections. In such three-tier architectures the pooled connections all log in to a database by using a single functional ID, and then manage all application users internally. When a user session needs access to the database, it acquires a connection from the pool, uses it and then releases it back to the pool. Guardium sees how the application interacts with the database, but it cannot attribute specific database actions to specific application users. For some widely used applications, Guardium has built-in support for identifying the end-user information from the application, and can relate database activity to the application end users.

- **[Identify Users with API](#)**

Some applications that manage users internally, cannot identify application user from the traffic. You can use the Application Events API to signal Guardium when a user acquires or releases a connection, or when any other event of interest occurs. The Application Events API provides simple calls that can be issued from within the application for this purpose.

- **[Identify Users via Stored Procedures](#)**

In many existing applications, all of the information needed to identify an application user can be obtained from existing database traffic, from stored procedure calls. Once Guardium knows what calls to watch for, and which parameters contain the user name or other information of interest, users can be identified automatically.

---

## Identify Users using the Application User Translation

Some applications manage a pool of database connections. In such three-tier architectures the pooled connections all log in to a database by using a single functional ID, and then manage all application users internally. When a user session needs access to the database, it acquires a connection from the pool, uses it and then releases it back to the pool. Guardium® sees how the application interacts with the database, but it cannot attribute specific database actions to specific application users. For some widely used applications, Guardium has built-in support for identifying the end-user information from the application, and can relate database activity to the application end users.

To use this function, follow these procedures:

1. Define an Application User Translation configuration for the application. See [Configure Application User Detection](#).
2. Populate any pre-defined groups that are required for that application. See [Populate Pre-defined Application Groups](#).
3. Create a report that includes the Application User Translation, using the APP\_USER\_NAME attribute in the App User Name Entity of the Access domain. Add the report(s) to your dashboard. There are predefined reports for EBS (EBS Application Access) and Peoplesoft (PSFT Application Access) that include this attribute. You can use these reports, or copy and modify them. See [Using the Query-Report Builder](#).

---

## Selective Audit Trail and Application User Translation

If the installed data access policy uses the selective audit trail feature to limit the amount of data logged, take note of these important considerations that apply to application user translation:

- The policy ignores all of the traffic that does not fit the application user translation rule (for example, not from the application server).
- Only the SQL that matches the pattern for that security policy is available for the special application user translation reports.

---

## Application user aliases

Each alias is a colon-separated string in the format **AppUserName :**

**Responsibility.** Responsibility can be empty. For example, the alias for APPLICATION USER is created by querying the Oracle Database server to get the App User Name. The Oracle Database server is defined in the GUI as either SERVER IP or Connect to Server IP if it is not empty. The Responsibility is based on the ID of the Value column (the DB\_VALUE of the ALIAS table in the format APPS\_CODE : ID).

---

## Oracle EBS with multiple interfaces

Guardium does not have specific pre-defined reports for Oracle EBS Application User Translation. Use the APP\_USER\_NAME in the Access domain to create your own reports.

When you add a new interface for an Oracle EBS server that is already defined, add another Data Source using the Connect to Server IP field. See step [13](#).

---

## Configure Application User Detection

1. Go to Protect > Database Intrusion Detection > Application User Translation. Details for existing application user translation configurations are displayed at the top of the page.

2. Type a unique code in the Application Code box.

Note: Under Central Management, you must use different application codes on different managed machines. This prevents aliases generated for the users from conflicting with each other. (Under Central Management, there is one set of aliases that is shared by all managed units.)

3. From the Application Type list, select the application type:
  - BO-WI - Business Objects / Web Intelligence
  - EBS - Oracle E-Business Suite
  - PeopleSoft
  - SAP Observed
  - SAP DB
  - SIEBEL Observed
  - SIEBEL DB
4. In the Application Version box, enter the application version number (11, for example).
5. From the Database Type list, select the database type. Only the types that are available for the selected Application Type and Version are displayed.  
Note: When the Application Type is set to EBS, SIEBEL DB, or SAP DB, you have the option of selecting from preexisting datasources by clicking Add Datasource. The datasource must match one of the supported database types for the application type being configured.
6. In the Server IP box, type the IP address the application uses to connect to the database.
7. In the Port box, type the port number the application uses to connect to the database.
8. In the Instance Name box, type the instance name the application uses to connect to the database.
9. In the DB Name box, type the database name for the application. (Required for some applications, not used for others.)
10. Check the Active box to enable user translation. Nothing is translated until after the first import of user definitions.
11. Enter a User Name for Guardium to use when accessing the database. Enter a password for Guardium to use when accessing the database.
12. Select the Responsibility box if you want to associate responsibilities (Administration, for example) with user names. Or clear the Responsibility box to just record user names. When the box is cleared, all activities performed by a user are grouped together, regardless of the responsibility at the time the activity occurred.
13. If the Application Type is EBS (Database Type is Oracle), two additional choices appear: Connect to Server IP and Connect to User Name. If populated, the system connects using that IP and username in order to retrieve the Responsibility and User Names. To support an Oracle Cluster Database that has multiple private/virtual interfaces for EBS connections and one public interface for the Guradium connection, create multiple "Application User Translation" configurations. For each configuration, enter one of the Virtual/Private interface IP addresses in the Server IP field and enter the public connected interface IP address to the Connect to Server IP field. Make sure this IP is connectable with Guardium and is able to retrieve the Responsibility and Application User Name.
14. Click Add to save the Application User Translation definition.
15. Continue to the procedure [Populate Pre-defined Application Groups](#)
16. Go to Manage > Activity Monitoring > Inspection Engines and click Restart Inspection Engines in the Inspection Engine Configuration panel.
17. Return to the Application User Translation page, click Run Once Now to import the user definitions for this application (and any others defined).
18. The data import of Application User Translation can be confirmed by looking at predefined reports, for example SAP Application Access. Go to Reports > Report Configuration Tools > Query-Report Builder and choose the report SAP Application Access. Regenerate this report and add to a pane, then set the date range to rather large (for example, go back a year for data).
19. In the Application User Translation page, click Modify Schedule to define an import operation to run on a regular basis. You should schedule the importing of user definition data at whatever interval is suitable for your environment. The maximum time that a new application user name is not available is the time between executions of the import operation. For instructions on how to use the scheduler, see [Scheduling](#)

Note: The first time Run Once Now is clicked after installing the Application User Translation setting(s), it retrieves the last update-date for the tables it looks at.

## Populate Pre-defined Application Groups

When Application User Translation has been configured, you must populate at least two pre-defined groups with information that is specific to your environment. This table identifies the groups that must be populated for each application type. For instructions on how to populate a group, see [Groups overview](#).

| Application | Pre-Defined Group  | Group Type |
|-------------|--------------------|------------|
| EBS         | EBS App Servers    | Client IP  |
|             | EBS DB Servers     | Server IP  |
| PeopleSoft  | PSFT App Servers   | Client IP  |
|             | PSFT DB Servers    | Server IP  |
|             | PeopleSoft Objects | Objects    |
| Siebel      | SIEBEL App Servers | Client IP  |
|             | SIEBEL DB Servers  | Server IP  |
| SAP         | SAP App Servers    | Client IP  |
|             | SAP DB Servers     | Server IP  |
|             | SAP - PCI          | Objects    |

## Unwilling to give DB\_USER PASSWORD for EBS application

In some cases you won't want to use the Oracle EBS DB\_USER for translating EBS traffic. In this scenario, when setting up Oracle EBS and wanting to translate traffic with Application User Translation, there are two choices to make it work:

- Supply the username and password that EBS uses to talk to Oracle (often APPS/\$passwd).
- If you don't want to provide the password the DB\_USER EBS uses to access Oracle, it is still possible to use Application User Translation, however the process is more complicated.

1. Make/choose a login for Oracle that permits access to the database for gathering aliases/users/responsibilities. That user needs access to the table [APPLSYS.FND\_USER and the view FND\_RESPONSIBILITY\_VL which combines two tables: APPLSYS.FND\_RESPONSIBILITY and APPLSYS.FND\_RESPONSIBILITY\_TL.

```
(CREATE VIEW FND_RESPONSIBILITY_VL AS SELECT /* $HEADER$ */ B.ROWID ROW_ID , B.WEB_HOST_NAME ,
B.WEB_AGENT_NAME , B.APPLICATION_ID , B.RESPONSIBILITY_ID ,
B.RESPONSIBILITY_KEY , B.LAST_UPDATE_DATE , B.LAST_UPDATED_BY ,
B.CREATION_DATE , B.CREATED_BY , B.LAST_UPDATE_LOGIN ,
B.DATA_GROUP_APPLICATION_ID , B.DATA_GROUP_ID , B.MENU_ID ,
B.START_DATE , B.END_DATE , B.GROUP_APPLICATION_ID ,
B.REQUEST_GROUP_ID , B.VERSION , T.RESPONSIBILITY_NAME ,
T.DESCRIPTION FROM FND_RESPONSIBILITY_TL T , FND_RESPONSIBILITY B
```

```
WHERE B.RESPONSIBILITY_ID = T.RESPONSIBILITY_ID
AND B.APPLICATION_ID = T.APPLICATION_ID
AND T.LANGUAGE = USERENV('LANG'))
```

2. Run the following SQL statements directly from the Oracle EBS system:  
`select RESPONSIBILITY_ID, RESPONSIBILITY_NAME from FND_RESPONSIBILITY_VL order by RESPONSIBILITY_ID; and select USER_ID, USER_NAME from FND_USER order by USER_ID;`

Once the user is set up so that those two statements successfully run, two different Application User Translation entries are needed. Both need to have the same server IP, port, and instance name, (and of course EBS and Oracle chosen for APP type and APP server type).

It does not matter if the Application Code is identical or not. One entry needs the username that EBS uses to connect to the database (usually APPS), but you can put in an incorrect (dummy) password. The second entry needs the username and password that has been created to access those tables.

3. Once both are entered with Active and Responsibility selected, click Run Once Now, and start or restart EBS (assuming that there is an Inspection Engine (S-TAP or net) looking at the traffic). The collection of data and the assignment of APPS user names to that data for the EBS traffic now takes place.

## Oracle privileges needed for the Oracle EBS App User

Translation:

1. Grant select on the following tables to Custom DB User:
  - APPLSYS.FND\_USER
  - APPLSYS.FND\_RESPONSIBILITY
  - APPLSYS.FND\_RESPONSIBILITY\_TL
2. Create a private synonym FND\_USER on APPLSYS.FND\_USER for Custom DB User.
3. Create a view called FND\_RESPONSIBILITY\_VL for Custom DB User. You can find this view under the APPS user to use as your template.

## How to Validate SAP Stack for Application User Translation

When supporting IBM® Guardium SAP Application User Translation, there is a difference between the ABAP Stack and Java™ Stack.

Note:

ABAP Stack and Java Stack have different kernel specifications.

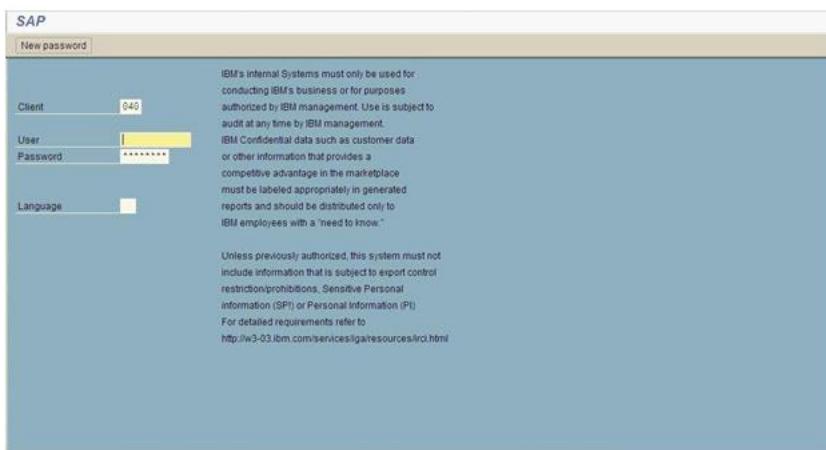
ABAP Stack and Java Stack systems have different tables.

ABAP Stack

Traditional ECC (Enterprise Core Components) SAP systems are written in ABAP code and are predominantly accessed via the SAP GUI, although web access is possible.

SAP ABAP systems have direct (read/write/update) access to traditional SAP databases. The databases are very large and contain all the sensitive data. This is where IBM Guardium is best utilized.

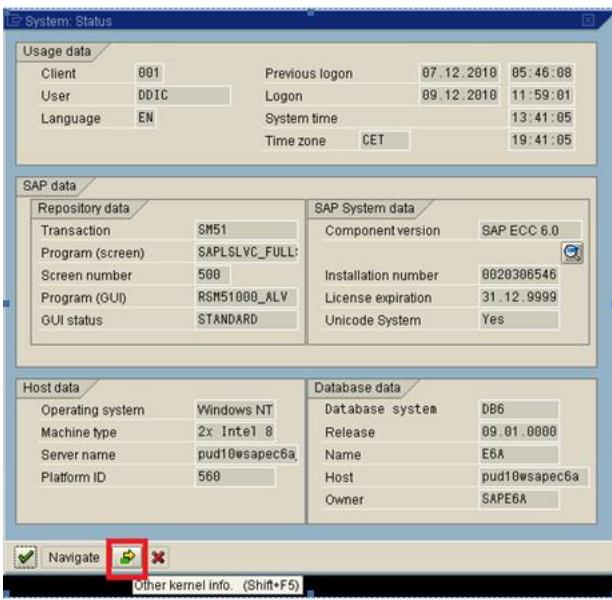
The following screen appears when you enter the SAP GUI (ABAP Stack):



1-SAP GUI (ABAP Stack)

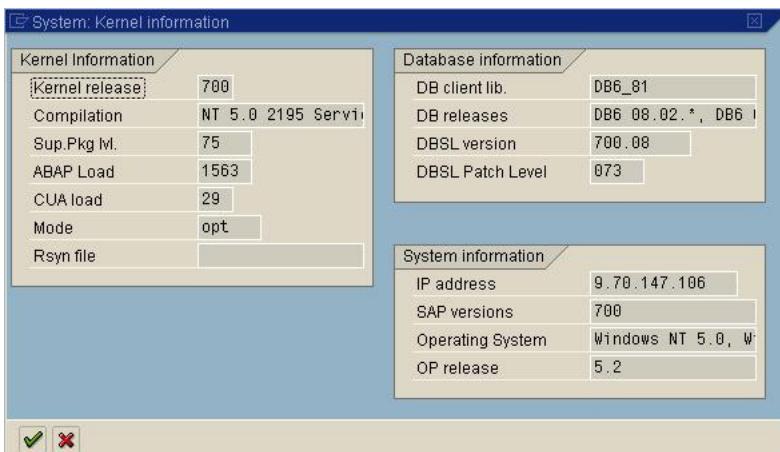
To validate the ABAP Stack SAP Kernel module for Application User Translation, follow these steps:

1. Log in to SAP.
2. Go to System > Status



2-System Status (ABAP Stack)

3. Click Other Kernel Info on the System Status screen.



3-System Kernel Information (ABAP Stack)

In this example, the kernel is 700.

SAP with a DB2® backend is also available for SAP kernel 640, but the user needs to set DB6\_DBDSL\_ACCOUNTING=1 (in kernel 700 and up, this DB6\_DBDSL\_ACCOUNTING value is 1 by default). SAP for Oracle backend requires a kernel of 710 or higher.

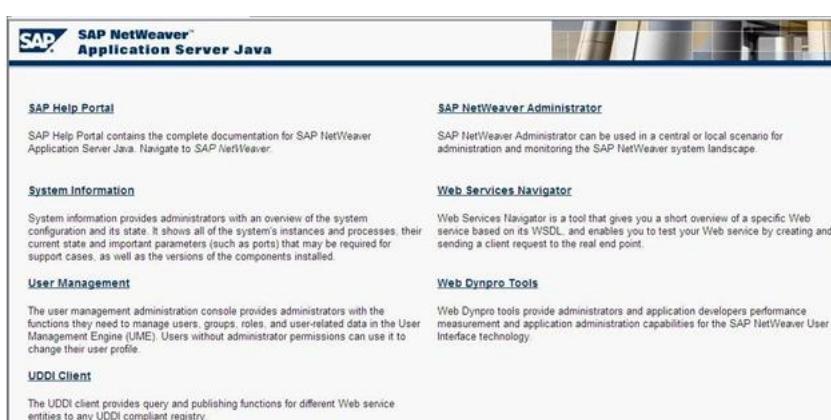
Data gets put into the app user field and the app event string.

Java Stack

SAP Portal systems are written in Java code and are the front end web applications utilizing pre-canned queries to display SAP related web pages.

Portal systems can only be accessed via a web browser. Portal system databases are much smaller with only a few tablespaces.

The following screen appears when you enter SAP Portal System (Java Stack).



#### 4-SAP Portal System (Java Stack)

To validate the Java Stack SAP Kernel module for Application User Translation, follow these steps: 1. Click on System Information.

The screenshot shows the SAP System Information interface with the 'System TCJ' tab selected. It displays detailed information about the system components:

- Message Server:** Host: magn13, Port: 2901, Type: DB2/AIX64 (SQL,09056).
- Enqueue Server:** Host: magn13, Port: 2021.
- Database:** Name: TCJ, Host: magn13, Type: DB2/AIX64 (SQL,09056).
- Software Components:** Name: sap.com/SAP-JECCOR, Version: 7.00 SP22 (1000.7.00.22.6.2010114162028), Applied: 2010523001119, License Number: 0020278108, System Number: 000000000310632781.
- Instance JC00:** Host: magn13, OS: AIX (ppc64) 5.3.
- dispatcher:** PID: 1002719, Node ID: 2919900, Name: IBM 39 VM, Vendor: IBM Corporation, Version: 2.3, JMI Parameters: Telnet Port: 50008.
- server01:** VM, system properties, Cluster, Node ID: 2919950, Kernel Version: 7.00 PatchLevel 97159.450.
- SDM:** VM, PID: 868526, SDM Port: 50018.

#### 5-System TCJ (Java Stack)

In this example, the SAP Kernel version is 7.00.

SAP for either Db2 or Oracle requires a kernel of 7.02 or higher.

SAP sets similar client properties in the Java stack as it did for ABAP Stack.

## Identify Users with API

Some applications that manage users internally, cannot identify application user from the traffic. You can use the Application Events API to signal Guardium® when a user acquires or releases a connection, or when any other event of interest occurs. The Application Events API provides simple calls that can be issued from within the application for this purpose.

Note: If your Guardium security policy has Selective Audit Trail enabled, the Application Events API commands that are used to set and clear the application user and/or application events are ignored by default, and the application user names and/or application events are not logged. To log these items so that they are available for reports or exceptions, include a policy rule to identify the appropriate commands, specifying the Audit Only rule action.

## GuardAppUser - Identify Users by API

Use two pre-defined triggers to set both Application User names and Application Event data.

- GuardAppEvent
- GuardAppUser

These each have start and stop triggers, and the Event has sub-triggers to set Type, Username, StrValue, NumValue, and Date.

The Guardium system is able to read special Select statements for the AppUserName and the AppEvent details.

The form is:

```
Select "action" [additional parameters] FROM [location]
```

Table 1. Action options

| Syntax                  | Action                                                         |
|-------------------------|----------------------------------------------------------------|
| GuardAppUser:<username> | Set GDM_CONSTRUCT_INSTANCE.APP_USER_NAME to <username>         |
| GuardAppUserReleased    | Clear APP_USER_NAME for subsequent queries                     |
| GuardAppEvent:Start     | Start a GuardAppEvent (and it looks for additional parameters) |
| GuardAppEvent:Released  | End a GuardAppEvent (clears info for subsequent queries)       |

Table 2. Additional parameters (which set the values in GDM\_APP\_EVENT)

| Parameters                             | Syntax                                           |
|----------------------------------------|--------------------------------------------------|
| GuardAppEventType: <event type string> | Set APP_EVENT_TYPE to <event type string>        |
| GuardAppEventUserName:<evntursname>    | Set GDM_APP_EVENT.APP_USER_NAME to <evntursname> |
| GuardAppEventStrValue:<strvalue>       | Set EVENT_VALUE_STR to <strvalue>                |
| GuardAppEventNumValue:<num>            | Set EVENT_VALUE_NUM to <num>                     |
| GuardAppEventDateValue:<date>          | Set EVENT_DATE to <date>                         |

Some examples of select statements follow:

Select guardappuser:tiberius from dual

Select guardappuserreleased from dual

Select GuardAppEvent:Start, GuardAppEventType:Event1, GuardAppEventUserName:Tiberius, GuardAppEventStrValue:abc, GuardAppEventNumValue:123, GuardAppEventDateValue:2016-01-26 15:55:28 from dual

Select GuardAppEvent:Released from dual

The FROM portion of the statement varies by database type.

Oracle: from DUAL  
Db2 from SYSIBM.SYSDUMMY1  
Informix from SYSTABLES  
MS-SQL <blank>  
Sybase <blank>  
MySQL either <blank> or from DUAL

## Guardium Identify App User name and Named Templates

---

There are several way to capture App User Name through Guardium. Guardium has two Turbine tables where APP\_USER\_NAME field values are stored, based on the way the data was received:

GDM\_CONSTRUCT\_INSTANCE  
GDM\_APP\_EVENT

The Named template %%AppUserName parameter in Guardium (see Global Profile menu) is mapped to the Turbine table, GDM\_CONSTRUCT\_INSTANCE. In order to use it in the Named Template, Guardium needs the APP\_USER\_NAME in the GDM\_CONSTRUCT\_INSTANCE table to be populated with the App User value.

Change the syntax of SQL command in the application to the following:

```
SELECT 'GuardAppUser:<value>'
```

This will put the values into the right table and this will replace the %%AppUserName parameter in the Named template with the right value.

Example

.....

```
select 'GuardAppUser:DB2_User' FROM SYSIBM.SYSDUMMY1 ;
select * from AppUser_DB2;
select 'GuardAppUserReleased' FROM SYSIBM.SYSDUMMY1 ;
select * from NoMoreUser_DB2;
```

.....

Look for the results in /var/log/messages file:

```
Jan 24 12:49:41 vx64 guard_sender[28274]: LEEF:1.0|IBM|Guardium|10.0|Alert per match|ruleID=20003|ruleDesc=Alert per match|severity=INFO|devTime=2016-01-24
11:50:39|serverType=DB2|classification=|category=|dbProtocolVersion=3.0|usrName=Db2_User|sourceProgram=DB2JCC_APPLICATION|start=1448383760000|dbUse=r=DB2INST1|dst=9.70.144.126|dstPort=50000|src=9.70.144.126|srcPort=58781|protocol=TCP|type=SQL_LANG|violationID=20|sql=select * from AppUser_DB2 FOR
READ ONLY|error=
```

## Set the Application User via GuardAppUser

---

Use this call to indicate that a new application user has taken control of the connection. The supplied application user name will be available in the Application User attribute of the Access Period entity. For this session, from this point on, Guardium will attribute all activity on the connection to this application user, until Guardium receives either another GuardAppUser call or a GuardAppUserReleased call, which clears the application user name.

To signal when other events occur (you can define event types as needed), use the GuardAppEvent call, described in the following section.

Syntax: `SELECT 'GuardAppUser:user_name' FROM location`

`user_name` is a string containing the application user name. This string will be available as the Application User attribute value in the Access Period entity.

`FROM location` is used only for Oracle, DB2®, or Informix®. (Omit for other database types.) It must be entered exactly as follows:

- Oracle: `FROM DUAL`
- Db2: `FROM SYSIBM.SYSDUMMY1`
- Informix: `FROM SYSTABLES`

Note: For Db2 for z/OS traffic, add a slash star comment enclosing 'GuardAppUser:user\_name' inside the SQL query. For example:

```
select /* 'GuardAppUser:user_name' */ col from tbl
```

## Clear the Application User via GuardAppUserReleased

---

Use the GuardAppUserReleased call to signal that the current user has relinquished control of the connection. Guardium will clear the application user name, which will remain empty for the connection until it receives another GuardAppUser call.

Syntax: `SELECT 'GuardAppUserReleased' FROM location`

`FROM location` is used only for Oracle, Db2, or Informix. (Omit for other database types.) It must be entered exactly as follows:

- Oracle: `FROM DUAL`
- Db2: `FROM SYSIBM.SYSDUMMY1`
- Informix: `FROM SYSTABLES`

## Set an Application Event via GuardAppEvent

---

This call provides a more generic method of signaling the occurrence of application events. You can define your own event types and provide text, numeric, or date values to be stored with the event, both when the event starts and when it ends. You can use this call together with the GuardAppUser call. Guardium will attribute all activity on the connection to this application event, until it receives either another GuardAppEvent:Start command or a GuardAppEvent:Released command.

Syntax:

```
SELECT 'GuardAppEvent:Start|Released',
'GuardAppEventType:type',
'GuardAppEventUserName:name',
'GuardAppEventStrValue:string',
'GuardAppEventNumValue:number',
'GuardAppEventDateValue:date' FROM location
```

Start | Released - Use the keyword Start to indicate that the event is taking control of the connection or Released to indicate that the event has relinquished control of the connection.

type identifies the event type. It can be any string value, for example: Login, Logout, Credit, Debit, etc. In the Application Events entity, this value is stored in the Event Type attribute for a Start call, or the Event Release Type attribute for a Released call.

name is a user name value to be set for this event. In the Application Events entity, this value is stored in the Event User Name attribute for a Start call, or the Event Release User Name attribute for a Released call.

string is any string value to be set for this event. For example, for a Login event you might provide an account name. In the Application Events entity, this value is stored in the Event Value Str attribute for a Start call, or the Event Release Value Str attribute for a Released call.

number is any numeric value to be set for this event. For example, for a Credit event you might supply the transaction amount. In the Application Events entity, this value is stored in the Event Value Num attribute for a Start call, or the Event Release Value Num attribute for a Released call.

date is a user-supplied date and optional time for this event. It must be in the format: yyyy-mm-dd hh:mm:ss, where the time portion (hh:mm:ss) is optional. It may be the current date and time or it may be taken from a transaction being tracked. In the Application Events entity, this value is stored in the Event Date attribute for a Start call, or the Event Release Date attribute for a Released call.

FROM location is used only for Oracle, Db2, or Informix. (Omit for other database types.) See the following example. However, any dummy table name is acceptable for the dummy SQL.

- Oracle: FROM DUAL
- Db2: FROM SYSIBM.SYSDUMMY1
- Informix: FROM SYSTABLES

The GuardAppEvent call populates an Application Events entity (see Application Events Entity in the Entities and Attributes section of the Appendices). When creating Guardium queries and reports, you can access the Application Events entity from either the Access Tracking domain or the Policy Violations domain.

If any Application Events entity attributes have not been set using the GuardAppEvent call, those values will be empty.

Regarding the two date attributes:

- Event Date is set using the GuardAppEvent call, or from a custom identification procedure as described in the following section.
- Timestamp is the time that Guardium stores the instance of the Application Event entity.

---

## Identify Users via Stored Procedures

In many existing applications, all of the information needed to identify an application user can be obtained from existing database traffic, from stored procedure calls. Once Guardium® knows what calls to watch for, and which parameters contain the user name or other information of interest, users can be identified automatically.

In the simplest case, an application might have a single stored procedure that sets a number of property values, one of which is the user name. A call to set the user name might look like this:

```
set_application_property('user_name', 'JohnDoe');
```

In a custom procedure mapping (described later), you can tell Guardium to:

- Watch for a stored procedure named set\_application\_property, with a first parameter value of user\_name.
- Set the application user to the value of the second parameter in the call (JohnDoe, in the example).

There may be multiple stored procedures for an application: one to start an application user session, one to end a session, and others to signal key events particular to that application. Guardium's custom identification procedure mechanism can be used to track any application events you want to monitor.

Since each of your applications may have a different way of identifying users, you may have to define separate custom identification procedure mappings for each application. To do that, follow the procedure outlined.

---

## Define a Custom Identification Procedure Mapping

1. Navigate to Protect > Database Intrusion Detection > Custom ID Procedures.
2. To view an existing mapping, hold the mouse pointer over the More Info column icon for the row containing the map you want to view.
3. To add a mapping, click Add.

4. In the Custom Map Name box, enter the name to be used for this mapping.
5. In the Procedure Name box, enter the name of the database procedure that will supply information.
6. Select Set or Clear from the Action list to indicate whether the procedure call will set or clear application values.
7. If application information can be obtained from an existing stored procedure call, but only under one or two conditions:
  - Use a Condition Location box to specify which stored procedure call parameter is to be tested
  - Use the corresponding Condition Value box to specify the value that must be matched to set application information from one or more of the other parameters.
  - For example, assume that a stored procedure named set\_context is used by an application to set a number of values, one of which is the user name. The procedure is passed three parameters: an application name, a property name, and a value. Three typical calls are illustrated:
    - set\_context('publishing\_application', 'role\_name', 'manager');
    - set\_context('publishing\_application', 'user\_name', 'jsmith');
    - set\_context('publishing\_application', 'company', 'guardium');
  - In the examples, the second statement illustrates the format of the call we are interested in. The second parameter (the property name) is the parameter that needs to be tested, so 2 would be entered in the Condition1 Location box, and user\_name in the Condition1 Value box.
  - If a second format of the call also sets the user name, then the Condition2 Location and Value boxes can be used. For example, assume that the following format of the procedure call is sometimes used to set a user name:
    - set\_context('admin\_application', 'admin\_name', 'wjones');
  - To use this procedure, to set the application user name, enter 2 in the Condition2 Location box, and admin\_name in the Condition2 Value box.

Note: If two conditions are used, the user name or any other information being extracted must be in the same parameter position for both types of calls.
8. For a Clear action:
  - To clear the application user only, set Application Username Position to 1 and all other positions to zero.
  - All other clear actions will clear the application event and the application user.
9. For a Set action, use the Parameter Position pane to indicate which stored procedure parameters map to which Guardium application event attributes. The first procedure parameter is numbered 1. Use 0 (zero – the default) for all attributes that are not set by the call. Application Username Position – Enter the parameter position of the application user name you want associated with database activity from this point forward (until reset, as described previously). Event String Value Position – Enter the parameter position of a string value for the event (for a login, this might be a user or account name). Event Number Value Position – Enter the parameter position of a numeric value for the event (for a transaction, this might be a dollar amount). Event Type Position – Enter the parameter position of a name for the event type (Login, Logout, Credit Request, etc.). Event Date Position – Enter the parameter position of a date/time value for the event. The format must be yyyy-mm-dd hh:mm:ss. The time portion (hh:mm:ss) is optional, and if omitted will be set to 00:00:00.

Note: If the Application Username Position is the only field configured and there is no current application event associated with this session, no new event will be created. Instead, the application user will be available in the Access Period Application User. If there is a current application event associated with this session, the application user will be updated in the Access Period Application User, and in a new application event.

10. In the Server Information pane: Select the database server type from the Server Type list. Enter the database user name in the DB Username box. Optional: Enter a database name in the Database Name box. If omitted, all databases will be monitored. Optional: Identify one or more servers. If no server is specified, all servers will be monitored. To select a specific server only, enter the server IP address and network mask in the Server IP and Server Net Mask boxes; or, to select a group of servers, select a server group from the Server IP Group list or click the Groups button to define a new group of servers.
11. When you are done, click the Add button to add the mapping to the list.
12. Reinstall the policy on the Guardium collector where you defined the custom ID procedure. The stored procedures will not be analyzed and processed by Guardium until the policy is reinstalled.

## Value Change Auditing

The Value Change Auditing feature tracks changes to values in database tables.

The Value Change Auditing feature tracks changes to values in database tables. For each table in which changes are to be tracked, you select which SQL value-change commands to monitor (insert, update, delete). Each time a value-change command is run against a monitored table, before and after values are captured. On a scheduled basis, the change activity is uploaded to a Guardium® system, where all the reporting and alerting functions can be used. The basic steps to perform to use the Value Change Auditing feature are:

1. Create an audit database on the database server. This database is where value-change data is stored until it is uploaded to the Guardium system. See [Creating an Audit Database](#).
2. Identify the tables to be monitored, and for each table select the value-change commands (insert, delete, update) for which changes will be recorded. To record the changes, a trigger is created for each table to be monitored, and that trigger writes the value-change data to the audit database. To allow updates to the audit database (by the trigger), all users with update privileges for the monitored table are given appropriate privileges for the audit database. This has implications for users who are given update privileges for that table later (see step 4). For detailed instructions on how to define the monitoring activities, see Define Monitoring Activities.
3. Schedule uploads to transfer value-change data from the database server to the Guardium system. See Schedule Value-Change Uploads.
4. Maintain audit database access privileges. After a trigger has been created, a new user may be given access to the table on which the trigger is based. If that user issues a monitored value-change command, it will fail because that user will not have appropriate privileges to update the audit database. See Maintain Privileged Users Lists.
5. Monitor change activity from the administrator console, or use the Value Change Tracking query domain to create custom reports on the Guardium appliance. See Value-Change Reporting.

## Define Monitoring Activities

After you define an audit database, use the Value Change Auditing Builder to identify the tables to be monitored, and to select the types of changes (inserts, updates, deletes) to be recorded.

1. Open the Value Change Auditing Builder by navigating to Harden > Configure Change Control (CAS Application) > Value Change Auditing Builder.
2. Click Add Datasource to open the Select datasource window.
3. Select a datasource on which an audit database is defined, or click  to define a new audit database. For information about defining an audit database, see [Creating an Audit Database](#).
4. Click Save to close the Select datasource window and add the selected datasource to the Value Change Audit page.
5. Optionally enter a Schema Owner and/or Object Name to limit the number of tables that are displayed when choosing the tables to be monitored. You can use the % (percent) wildcard character. For example, to limit the display to all tables that begin with the letter a, enter a% in the Object Name box.
6. Click Choose Tables To Monitor to open the Define Data Audit panel.

7. Mark the Select box for each table to be monitored.

Attention: For Microsoft SQL Server, Sybase, and Sybase IQ, the Guardium system does not receive audit updates to any column that is a primary key or part of a composite key.

Note: You cannot define a trigger for a table that contains one or more user-defined data types.

The Trigger Defined column indicates if a trigger is already defined for the table. The Audit Insert, Audit Delete, and Audit Update check boxes indicate if the trigger will record changes for that command.

If the Trigger Defined column is not marked, marking the Select checkbox for a table automatically marks all three the Audit checkboxes (Audit Insert, Audit Delete, and Audit Update). If you do not want to monitor one or two of those commands, clear the appropriate checkbox.

8. Click Add Selections to define triggers for the selected tables. You will be informed of the action taken.

9. Click OK to close the message box and re-display the Define Data Audit panel. The selected tables remain selected, and the Trigger Defined column is now marked for those tables. Note: The instant a trigger is defined for a table, it is active and recording changes for the selected commands in the audit database. The configuration of triggers is done entirely on the database server, which is unlike most other Guardium configurations, which are defined on the Guardium database, and then activated or deactivated as a separate task.

10. To define additional actions, repeat these steps, or remove triggers by marking the appropriate Select check boxes and clicking Remove Selections.

11. Click Done after you complete all changes.

Note: The Cancel button does not back out any changes that you have made to triggers using the Add or Remove Selections buttons.

## After Defining Monitoring Activities

---

If you have added value-change monitoring activities to a datasource for the first time, you should schedule uploads for this datasource, because the audit database will be emptied only after the data recorded there has been uploaded to the Guardium system. See the next section.

## Schedule Value-Change Uploads

---

1. Open the Value Change Auditing Builder by navigating to Harden > Configure Change Control (CAS Application) > Value Change Auditing Builder.

2. Select the audit datasource for which you want to schedule uploads, and click Schedule Upload to open the general-purpose task scheduler. If you need help defining a schedule, see Scheduling in the Common Tools book.

## Maintain Privileged Users Lists

---

When the value-change feature adds a trigger for a database table, all current users with permission to update that table are granted permission to update the audit database table. This is required because the trigger updates the audit database with new and/or old values. If a new user is granted update permission for a monitored table, when that user attempts an update, the update is not allowed because that user does not also have permission to update the audit database. When this happens, you must update the audit database privileged users list by using the Value Change Auditing Builder.

To update the audit database privileged users list, the database user ID that is used to log in to the monitored database must be the creator of any role to which new users have been added. Otherwise, the members of that role will not be available.

1. Open the Value Change Auditing Builder by navigating to Harden > Configure Change Control (CAS Application) > Value Change Auditing Builder.

2. Click Add Datasource to open the Select datasource window. Select the appropriate datasource from the list, and click Save.

3. Click Update Audit Tables Privileged Users. The permissions for all users who can run triggers to update the audit database tables are updated, and you are informed when the operation completes.

4. Click OK to close the message box.

## Value-Change Reporting

---

You can view value-change data from the default Values Changed report, or you can create custom reports using the Value Change Tracking domain. By default, the Value Change Tracking domain is restricted to users having the admin role.

## Values Changed Default Report

---

There is one default values-changed report available by navigating to Reports > Real-Time Guardium Operational Reports > Values Changed.

The main entity for the Values Changed report is the Changed Columns entity. In most cases, there is a separate row of the report for every column change that is detected for every audit action (Insert, Update, Delete). However, for MS SQL Server and Sybase, if the monitored table does not have a primary key, there are two rows per change, with the old and new values displayed on separate rows.

## Creating an Audit Database

---

Create an audit database and perform value-change monitoring activities.

To create an audit database and perform value-change monitoring activities, you must have a user account with appropriate permissions to:

- Create a database on the server
- Create a database user account on the server

Log in to each database to be monitored Create tables and triggers on each database to be monitored

## Before Defining an Audit Database under Informix or Sybase

---

For Informix® and Sybase (except for Sybase IQ, which does not support triggers) and depending on the operating system for the database server, you must perform one of the following procedures before defining the audit database.

## Informix Setup - Locate or Create a New Database Space

---

This topic applies for Informix (9.4 or later). Under Informix, we strongly recommend that you avoid using the default root database space, root\_dbs. You cannot drop this space or reduce its size.

You should use any other database space that has been defined, or to create a new database space, perform one of the following procedures (depending on the operating system).

## Informix - Create an Informix Database Space on a Windows Server

---

This procedure is performed outside of the Guardium® GUI, and applies for Informix version 9.4 or later.

1. Verify that the database server is online and listening.
2. Create a zero-byte file named guardium\_dbs\_dat.000 in the C:\IFMXDATA\server-name directory (server-name is the name of the Informix server or the service name). You can do this by saving an empty text file, and then renaming the file, replacing the txt suffix with 000.
3. Make the following directory the working directory:  
C:\Program Files\Informix\bin
4. Execute following command:

```
C:\Program Files\Informix\bin>onspaces -c -d guardium_dbs -p C:\IFMXDATA\server-name\guardium_dbs_dat.000 -o 0 -s 150000
```

If the file is created successfully, you see the following messages:

```
Verifying physical disk space, please wait ...
Space successfully added.
** WARNING ** A level 0 archive of Root DBSpace will need to be done.
```

5. Restart the Informix server, and use a suitable tool (Aqua Data Studio remote client, for example) to connect and verify that the space named guardium\_dbs has been created. Your first connection attempt may fail with a message about the server running in Quiescent Mode. If this happens, attempt to re-connect at least two more times, and it should work.
6. To verify that the guardium\_dbs database space has been created, use Aqua Data Studio, and look under Storage.

## Informix - Create an Informix Database Space on a Unix Server

---

This procedure is performed outside of the Guardium GUI, and applies for Informix version 9.4 or later.

1. From a command-line window, enter the following commands:

```
su - informix
cd demo/server
vi guardium_dbs
```

2. Without adding any text, save the empty guardium\_dbs file.
3. Enter the following commands:

```
chmod 660 guardium_dbs
cd ../../bin
onspaces -c -d guardium_dbs -p /home/informix10/demo/server/guardium_dbs -o 0 -s 100000
```

## Sybase Setup - Initialize Disks

---

This topic applies for Sybase servers only (except for Sybase IQ, which does not support triggers). Depending on the operating system of the database server, perform one of the following procedures to initialize disks.

## Sybase - Initialize Disks on a Windows Sybase Server

---

1. Connect to the server on which you want to create the Guardium audit database: guardium\_audit.
2. Create a folder named guardium\_audit, under the c: drive.
3. Connect to the database.
4. Execute the following commands:

```
use master
go
disk init name="guardium_auditdev", size=8192
go
disk init name="guardium_auditlog",
physname="c:/guardium_audit/guardium_auditlog", size=8192
go
```

## Sybase - Initialize Disks on a Unix Sybase Server

---

1. Connect to the database.
2. Execute the following statements:

```
use master
go
disk init name = 'guardium_auditdev', physname
=''/home/sybase/data/guardium_auditdev' , size = 8192
go
disk init name = 'guardium_auditlog', physname
=''/home/sybase/data/guardium_auditlog' , size = 8192
go
```

## Create the database

---

For an Informix or Sybase database, be sure to perform the preliminary tasks before performing this procedure.

1. Open the Value Change Database Builder by navigating to Harden > Configuration Change Control (CAS Application) > Value Change Audit Database Creation.

2. Click Add Datasource to open the Select datasource window.

Datasources that are defined from the Value Change Auditing application are labeled Monitor Values. Datasources that are defined for other applications have different labels (such as Listener, or DBAnalyzer). The other datasources may not have the appropriate set of database access permissions for that Value Change

Auditing application, which requires a user account with database administrator authority. If a suitable datasource is not available, click to define a database to monitor. For information about defining datasources, see [Creating a datasource definition](#).

Note: If a GUARDIUM\_AUDIT database already exists on this dbserver, you cannot create another one. You must drop the GUARDIUM\_AUDIT database/user before you create a new one.

3. Select a datasource that uses an administrator account, and click Save to add it to the Datasources window on the Create Value Change Audit Database page.
4. Enter an Audit Datasource Name. This is the name that identifies the datasource later, to define monitoring tasks and to upload data. Do not confuse this name with the name of the Datasource from the Datasources panel.
5. Optionally select Share Datasource to share this datasource with other applications (Classification, for example). The default is not to share the datasource. This type of datasource requires administrator privileges, so you may not want to share this datasource with other applications.

Note: To share a datasource with other users, assign security roles to that datasource.

6. For any database type other than DB2®, there are additional fields in the Audit Configuration pane. All fields are required. Referring to the following table, enter the appropriate values.

Table 1. Additional Audit Configuration Fields Table

| Database Type | Field: Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Informix      | <b>Database Space:</b> Enter the name of an existing database space to use, or enter the name of the database space you created for the audit database (guardium_dbs in the example shown previously). If you leave this blank, the default root_dbs space will be used, which we do not recommend.                                                                                                                                                                                                                                                                                                                                                                                  |
| MS SQL Server | <b>Audit User Name:</b> Enter a new database user name to use when accessing the audit database. This user will be given the sysadmin role.<br><br><b>Audit Password:</b> Enter a password.<br><br>An additional choice appears in Value change Audit Database Creation menu screen when then the datasource is MSSQL server. This additional choice appears only when the datasource is MSSQL Server.<br><br>Compatibility Mode: Choices are Default or MSSQL 2000. The processor is told what compatibility mode to use when monitoring a table.<br><br>Use the GuardAPI command, <code>grdapli list_compatibility_modes</code> to show the compatibility modes for MS SQL Server. |
| Oracle        | <b>Audit Password:</b> Enter the password for the system user, which will be the database account used to access the audit database.<br><br><b>Default Tablespace:</b> Enter a name for the default tablespace.<br><br><b>Temp Tablespace:</b> Enter a name for the temporary tablespace.                                                                                                                                                                                                                                                                                                                                                                                            |
| Sybase        | <b>Audit User Name:</b> Enter a new database user name to use when accessing the audit database. This user will be granted the sa_role.<br><br><b>Audit Password:</b> Enter a password.<br><br><b>Data Device Name:</b> Enter the same data device name used when initializing the disk for the audit database (guardium_auditdev in the disk initialization procedure described earlier).<br><br><b>Log Device Name:</b> Enter the same log device name used when initializing the disk for the audit database (guardium_auditlog in the disk initialization procedure described earlier).                                                                                          |

7. Click Create Audit Database to create the audit database.

8. Use the selection Value Change Audit Database Update and Upload on the Config and Control tab to select the actions in this table.

Restriction: For Microsoft SQL Server, Sybase, and Sybase IQ, the Guardium system does not receive updates to any column that is a primary key or part of a composite key.

| Action          | Description                                                                  |
|-----------------|------------------------------------------------------------------------------|
| Delete          | Click to remove the datasource from the Datasources pane.                    |
| Modify          | Click to edit this datasource definition in the Datasource Definition panel. |
| Schedule Upload | Click to schedule the upload of this audit datasource.                       |

## What to do next

---

After you create an audit database on a database server, it is available for use by the Value Change Auditing Builder for building triggers. For more information, see [Value Change Auditing](#).

## Monitored Table Access

---

This feature adds a “Last Assessed” field to relevant tables, for interaction with Optim Designer data lifecycle products.

This feature is also called “Table Last Referenced”.

This feature uses Guardium’s External Feed that is preconfigured with the data (a predefined External Feed map), and an audit process to run it.

## Follow these Steps

---

1. Create the target (Optim) tables on any Informix® database. Use the script.

2. Open the Audit Process Builder by navigating to Comply-> Tools and Views-> Audit Process Builder, then edit the process named Table Last Referenced. Add a datasource to the External Feed task (the Informix datasource that contains the tables) and setup the run-time parameter for servers group. All the rest is predefined and there is no need to change it.
3. Run (or schedule to run periodically) the audit process.

Note: The resulting table will show only the last run. The receiver count is the count of the receivers, and not the count of run results since the last run only. IBM® Guardium® can detect external references to database objects, specifically tables. This capability, in conjunction with Optim Designer, can be used to manage the retirement of inactive tables or archiving with certain retention policies.

Guardium collects and maintains a list of tables with the date of last reference. The list is built using policies in Guardium that dictate the interval of last reference and the frequency to be used for updating the list content. The information captured by Guardium is referred to as the "last reference" list and supplies the following information: What tables are no longer referenced? What table access trends exist for retirement candidates?

Having the ability to accurately plan for the retirement of applications will help to:

- Plan for hardware retirement or redeployment
- Reduce cost of ownership by moving or retiring those resources supporting the applications (for example, hardware, DBA(s), Application owners, IT operations such as backups).
- Know what tables are rarely or never accessed

This functionality of IBM Guardium has been added directly to the Optim Designer user interface.

The information supplied by Guardium to Optim consists of the following attributes per table entry:

**Table 1. Monitored Table Access List Entry**

| List Entry     | Description                                          |
|----------------|------------------------------------------------------|
| Field          | Comment                                              |
| DataSourceDesc | Description                                          |
| Server IP      |                                                      |
| Host Name      |                                                      |
| DB Vendor      | for example, Oracle, DB2®                            |
| User Name      | for example, for Oracle it mostly defines the schema |
| Database Name  |                                                      |
| Schema         |                                                      |
| Table          |                                                      |
| Date           | Date of last access                                  |

## Script to create Informix tables in the Optim product

---

```
Last_referenced_datasource
create table last_referenced_datasource (
 id serial(1) not null,
 datasource_desc varchar(100),
 server_ip char(39),
 host_name varchar(200),
 db_vendor char(40),
 primary key (id) constraint last_referenced_datasource_pk
);

Last_referenced_table
create table last_referenced_table (
 id serial(1) not null,
 datasource_id int not null,
 user_name char(32),
 db_name char(128) not null,
 schema_name char(128) not null,
 table_name char(128) not null,
 last_reference datetime year to second not null,
 primary key (id) constraint last_referenced_table_pk,
 foreign key (datasource_id) references last_referenced_datasource(id) constraint last_referenced_table_fk
);
```

---

## Installing and activating the FamMonitor on Windows servers

The FamMonitor enables monitoring and collection of audit information and policy rules, and real time alerts or blocking of suspicious users or connections on your Windows servers. You can install it by command line, the wizard, or GIM.

- [Install the FamMonitor installation package with the wizard](#)  
Use the wizard to install the FamMonitor installation package on your Windows database.
- [Install the FamMonitor bundle with GIM](#)  
Install the GIM client on the Windows server, then use it to install the FamMonitor.
- [FamMonitor GIM installation parameters](#)  
Understand the parameters that you can use in your GIM installation of the FamMonitor bundle.
- [Install and uninstall the FamMonitor installation package with command line](#)  
Use the command line installation to install the FamMonitor installation package on your Windows database.
- [FamMonitor command line installation parameters](#)  
Understand the parameters that you can use in your script installation of the FamMonitor installation package.

## Related concepts

---

- [Investigation Dashboard for files](#)

## Related tasks

---

- [Enabling File Activity in the investigation dashboard](#)

## Related reference

---

- [File Activity Monitor APIs](#)

## Install the FamMonitor installation package with the wizard

Use the wizard to install the FamMonitor installation package on your Windows database.

### Before you begin

---

- The FamMonitor installation package must be accessible. Download from [Fix Central](#) or obtain from your Guardium representative.
- If S-TAP is installed, it is V11.0 and higher.

### Procedure

---

1. Log on to the database server using a system administrator account.
2. Unload and unzip the FamMonitor installation package on the database.
3. Double-click Setup.exe to open the wizard.
4. Accept the licensing agreement and click Next.
5. Follow the prompts. Most customers prefer Setup type as Typical. The custom setup gives a custom install directory.  
Use the Appliance Address(es) field to type in additional Guardium® hostnames or IP addresses. If there is a failover, the FAM agent attempts to connect to the next appliance on the list.
6. When the installation is complete, click Finish to close the installer.
7. On the Guardium system, in the Windows Services, verify that IBM Security Guardium FAM for Windows is Running.
8. On the Guardium GUI , in the S-TAP Control page, verify that the FAM Status is active.

### Results

---

Monitoring and collection of audit information and policy rules starts, enabling real time alerts or blocking of suspicious users or connections.

## Install the FamMonitor bundle with GIM

Install the GIM client on the Windows server, then use it to install the FamMonitor.

### Before you begin

---

- FamMonitor bundle is uploaded on the GIM server. The FamMonitor bundle name starts with: FAMMONITOR
- The GIM client is installed on the file server.
- If S-TAP is installed, it is V11.0 and higher.

### About this task

---

All GIM parameters for FamMonitor start with FAMMONITOR\_.

### Procedure

---

- Verify that the GIM client is installed on the database server. See [Installing the GIM client on a Windows server](#).
  - Upload the FAM bundle to the GIM server.
    - Go to Manage > Module Installation > Upload Modules.
    - Click Choose File and select the FAM bundle that you want to install.
    - Click Upload to upload the module to the appliance.

The module appears in the Import Uploaded Modules table.

    - In the Import Uploaded Modules table, click the check box next to the FamMonitor bundle you want to install.

The bundle imports and becomes available for installation. The Upload Modules page resets and the Import Uploaded Modules table is now empty.
  - Navigate to Manage > Module Installation > Set up by Client.
  - In the Choose clients section, select the database servers where you want to install the FamMonitor. Select individual clients using check boxes in the table, or use the Select client group menu to select a group of clients. Click Next to continue.
  - In the Choose bundle section, use the Select a bundle menu to select the FamMonitor bundle.
- After selecting a software bundle, the Selected bundle action column indicates Install, the action that will be performed for each client:
- Attention:
- By default, the Select a bundle menu shows only the latest uploaded bundle version regardless of platform or compatibility with selected clients. To install a different bundle version for a specific platform or client, clear the Show only latest versions check box and select the required bundle.
  - If you upload and import new bundles while using the Set up by Client tool, refresh the browser to see the new bundles.
  - If you already have a bundle scheduled for installation, installing a new bundle removes the existing schedule.
- Click Next to continue.
6. In the Choose parameters section, specify values for required and optional parameters. Use the or to add or remove optional parameters. Use the to search for parameters by name or description.
- Important: Unless identified as a client-specific parameter, values provided in the Choose parameters section are applied to all client installations. For client-specific parameters, the value field is disabled and values are defined per-client in the Configure clients section.
- Click Next to continue.
7. In the Configure clients section, use the table to review and edit parameter values for each client.
- Editable parameters show a icon next to the parameter value. Click the icon to edit the value.
- When installing on a Central Manager, you must provide a value for FAMMONITOR\_SQLGUARD\_IP
  - When installing on a Collector: GIM, by default, takes the GIM client values for FAMMONITOR\_TAP\_IP and FAMMONITOR\_SQLGUARD\_IP. You do not need to assign any other parameter values. The GIM client values are GIM\_CLIENT\_IP and GIM\_URL, respectively.
- Configure additional parameters as relevant. See full parameter list in [FamMonitor GIM installation parameters](#).
- Note: You can also configure GIM parameters using the grdapi command: `gim_update_client_params`.
8. Click Install to begin the software installation. Use the icon to schedule the installation, then click OK to continue.

## Results

Monitoring and collection of audit information and policy rules, enabling real time alerts or blocking of suspicious users or connections.

## Related concepts

- [High level workflow for file activity monitoring](#)
- [Using GuardAPI](#)

## Related tasks

- [GIM Set up by Client](#)

## Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

## FamMonitor GIM installation parameters

Understand the parameters that you can use in your GIM installation of the FamMonitor bundle.

Table 1. FamMonitor GIM installation parameters

| GIM parameter                      | Description                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FAMMONITOR_SQLGUARD_IP             | The Guardium IP.                                                                                                                                                                                                                                                                                                                                                                |
| FAMMONITOR_ADDITIONAL_SQLGUARD_IPS | Additional Guardium® hostnames or IP addresses. If there is a failover, the FAM agent attempts to connect to the next appliance on the list.                                                                                                                                                                                                                                    |
| FAMMONITOR_ENABLED                 | <ul style="list-style-type: none"> <li>0: FamMonitor is stopped after installation.</li> <li>1: FamMonitor is started after installation.</li> </ul>                                                                                                                                                                                                                            |
| FAMMONITOR_FAM_NORDP               | Determines whether Guardium records the remote client IP address or the server IP address as the client IP address in its file events, for users connected by remote desktop. <ul style="list-style-type: none"> <li>0: Guardium records the remote client IP address.</li> <li>1: Guardium records the server IP address as the client IP address.</li> </ul> <p>Default=0</p> |
| FAMMONITOR_INSTALL_DIR             | Required. This is the install directory. The default install path is program files\ibm\fammonitor                                                                                                                                                                                                                                                                               |
| FAMMONITOR_INSTALLER_LOG_DIR       | Specifies the location for storing the FamMonitor installer log files. Use this parameter if you want don't want to use the default location (C:\Program Files\IBM\Windows Fam Monitor).                                                                                                                                                                                        |

| GIM parameter       | Description                                                                                                                  |
|---------------------|------------------------------------------------------------------------------------------------------------------------------|
| FAMMONITOR_TAP_IP   | The local/client IP. Required for unattended installation.                                                                   |
| FAMMONITOR QUIET    | Install silently. (Does not require a value.)                                                                                |
| FAMMONITOR_CMD_LINE | Adds key and value to Famonitor config file. Format: key1=value1 key2=value2, separated by space between pairs of key-value. |

## Install and uninstall the FamMonitor installation package with command line

Use the command line installation to install the FamMonitor installation package on your Windows database.

### Before you begin

- The FamMonitor installation package must be accessible. Required for file monitoring. Download from [Fix Central](#) or obtain from your Guardium representative.

### Procedure

- Log on to the database server using a system administrator account.
- Copy the installation package to your database, and using the Windows Command Prompt, navigate to the Windows FAM installer directory.  
For example,

```
cd c:\Windows-FamMonitor-V11.0.0.nn
```

You should find a **setup.exe** executable in the installation package directory.

- Install FamMonitor using the **setup.exe** executable with the appropriate parameters.

The required parameters are:

- TAPHOST
- APPLIANCE
- UNATTENDED

All parameters except INSTALLPATH can be updated after the installation. A typical install command is:

```
setup.exe -UNATTENDED -APPLIANCE 10.0.147.234 -TAPHOST 10.0.145.41
```

where:

- UNATTENDED (required) invokes the command-line installer.
- APPLIANCE specifies the IP address of the Guardium® system that will control the FamMonitor.
- TAPHOST (required) specifies the client IP address where the FamMonitor is being installed.

Optional parameters:

- INSTALLPATH
- CUSTOMER
- COMPANY
- SERVICEUSER
- SERVICEPASSWORD
- START: 0 means the FAM monitor service is stopped after install

Mandatory parameter for **uninstall**:

- UNINSTALL

For a complete description of the parameters, see [FamMonitor command line installation parameters](#).

### Results

Monitoring and collection of audit information and policy rules starts, enabling real time alerts or blocking of suspicious users or connections.

## FamMonitor command line installation parameters

Understand the parameters that you can use in your script installation of the FamMonitor installation package.

Install the FamMonitor installation package using the **setup.exe** executable with the relevant parameters, in this format:

**Setup.exe -PARAMETER value**

Do not use "=" sign to assign values to the parameters.

Table 1. FamMonitor command line installation parameters

| Command line parameter | Description                                                                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| APPLIANCE              | Required. The Guardium IP. You can set up multiple appliances by specifying this parameter multiple times, each with a unique value.                                                     |
| COMPANY                | Specify to change the company name.                                                                                                                                                      |
| CUSTOMER               | Specify to change the customer name.                                                                                                                                                     |
| INSTALLERLOGPATH       | Specifies the location for storing the FamMonitor installer log files. Use this parameter if you want don't want to use the default location (C:\Program Files\IBM\Windows Fam Monitor). |
| INSTALLPATH            | This is the install directory. The default install path is program files/ibm/fammonitor.                                                                                                 |

| Command line parameter | Description                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NORDP                  | Determines whether Guardium records the remote client IP address or the server IP address as the client IP address in its file events, for users connected by remote desktop. <ul style="list-style-type: none"> <li>• 0: Guardium records the remote client IP address.</li> <li>• 1: Guardium records the server IP address as the client IP address.</li> </ul> Default=0 |
| SERVICEUSER            | Specifies the service user account.                                                                                                                                                                                                                                                                                                                                          |
| SERVICEPASSWORD        | The password for the user.                                                                                                                                                                                                                                                                                                                                                   |
| START                  | <ul style="list-style-type: none"> <li>• 0: FamMonitor is stopped after installation</li> <li>• 1: FamMonitor is started after installation.</li> </ul>                                                                                                                                                                                                                      |
| TAPHOST                | Required for unattended installation. The local/client IP.                                                                                                                                                                                                                                                                                                                   |
| UNATTENDED             | Required. Install silently. (Does not require value.)                                                                                                                                                                                                                                                                                                                        |
| UNINSTALL              | Uninstalls the FamMonitor. A value is not required.                                                                                                                                                                                                                                                                                                                          |

## File Activity Monitor for NAS and SharePoint

The Guardium File Activity Monitor (FAM) monitors activity across files and directories residing on NAS devices and SharePoint servers in the Windows environment.

NAS or network-attached storage is a file-level storage system based on networked appliances containing multiple storage devices. SharePoint is a web-based collaborating platform and a document management & storage system.

FAM's ability to monitor these environments enables users to identify threats and streamline operations.

Use the following work flow to enable File Activity Monitoring across your NAS devices or SharePoint environment.

- [Supported platforms for file activity monitoring](#)
- [Monitoring Permissions](#)  
Enable these permissions to allow file activity monitoring on your NAS or SharePoint environments.
- [Installation](#)  
Use these instructions to install the File Activity Monitor (FAM) on your NAS or SharePoint environment.
- [Configuration](#)  
After installing, configure the File Activity Monitor (FAM) to begin monitoring your NAS or SharePoint environment.
- [Viewing Results](#)  
To view file activity on your NAS device, use the NAS File Activities report. For SharePoint, use the SharePoint File Activities report.
- [Uninstallation](#)  
Uninstall the File Activity Monitor (FAM) for network-attached storage (NAS) devices or SharePoint by using the Windows Control Panel.

## Supported platforms for file activity monitoring

For the list of supported platforms for files, see [Guardium Supported Platforms for Files](#).

## Monitoring Permissions

Enable these permissions to allow file activity monitoring on your NAS or SharePoint environments.

### NAS Permissions

#### NetApp Data ONTAP Cluster-Mode Permissions

The policy name and credentials are case-sensitive when targeting a NetApp Data ONTAP Cluster-Mode device. The policy name must be `StealthAUDIT` and the engine name must be `StealthAUDITEngine`. A tailored FPolicy is recommended as it decreases the impact on the NetApp device.

The credential that is associated with the FPolicy used to monitor activity must be provisioned with at least the following CLI commands:

| CLI command | Access   |
|-------------|----------|
| version     | Readonly |
| volume      | Readonly |
| vserver     | Readonly |

For more options to enable and configure the FPolicy, use the following CLI commands:

#### Employing the “Enable and connect FPolicy” Option.

The File Activity Monitor can be configured to ensure that everything is actively monitored with periodic checks on the FPolicy. If the “Enable and connect FPolicy” option is enabled, then the credential requires the following permissions to enable the FPolicy, connect to the FPolicy, and collect events:

| CLI Command | Access   |
|-------------|----------|
| version     | Readonly |
| volume      | Readonly |

| CLI Command                    | Access   |
|--------------------------------|----------|
| vserver                        | Readonly |
| vserver fpolicy disable        | All      |
| vserver fpolicy enable         | All      |
| vserver fpolicy engine-connect | All      |

#### Employing the “Configure FPolicy” Option

The File Activity Monitor can automatically configure FPolicy. If the “Configure FPolicy” option is enabled, then the credential requires the following permissions to enable the FPolicy, connect to the FPolicy and collect events:

| CLI command                                                           | Access   |
|-----------------------------------------------------------------------|----------|
| version                                                               | Readonly |
| volume                                                                | Readonly |
| vserver                                                               | Readonly |
| server fpolicy                                                        | All      |
| security certificate install (only needed for FPolicy TLS connection) | All      |

#### NetApp Data ONTAP 7-Mode Permissions

It is necessary to enable the “file and printer sharing” where FAM is installed.

An FPolicy must be configured on the target device for file activity monitoring. A tailored FPolicy is recommended as it decreases the impact on the NetApp device. The credential associated with the FPolicy used to monitor activity must be provisioned with access to the following API calls:

- login-http-admin api-system-api-list
- api-system-get-version
- api-cifs-share-list-iter-\* api-volume-list-info-iter-\*

If the File Activity Monitor will be automatically configuring the FPolicy, then the following command is also needed:

- api-fpolicy\*

If the File Activity Monitor will be configured to use the “Enable and connect to the FPolicy” option, then the following command is also needed:

- cli-fpolicy\*

The credential must also have the following permissions on the target device:

- Group membership in both of the following groups:
- ONTAP Power Users
- ONTAP backup Operators

#### EMC Celeraic or Unity device

The EMC Common Event Enabler (CEE) should be installed on the Windows proxy server where FAM agent is deployed.

#### EMC Isilon device

The EMC Common Event Enabler (CEE) should be installed on the Windows proxy server where the File Activity Monitor agent is deployed.

#### Hitachi

A Hitachi device can host multiple Enterprise Virtual Servers (EVS). Each EVS has multiple file systems. Auditing is enabled and configured per file system. HNAS generates the audit log files in EVT format (a standard event log format in Windows XP/2003 and earlier). Hitachi stores the generated audit logs in a user specified location on the file system. FAM accesses this location to collect the log files as they are generated. The credential used to monitor activity must be provisioned with:

- Capability of enabling a File System Audit Policy on the Hitachi device
- Audit rights to the Hitachi log directory

## Firewall rules - Windows Proxy Server

#### NetApp Data ONTAP Cluster-Mode Firewall Rules

The following firewall settings are required for communication between FAM and the NetApp Data ONTAP Cluster-Mode device:

| Communication Direction | Protocol         | Ports | Description    |
|-------------------------|------------------|-------|----------------|
| FAM to NetApp           | HTTP (Optional)  | 80    | ONTAPI         |
| FAM to NetApp           | HTTPS (Optional) | 443   | ONTAPI         |
| NetApp to FAM           | TCP              | 9999  | FPolicy events |

#### NetApp Data ONTAP 7-Mode Firewall Rule

The following firewall settings are required for communication between FAM and the NetApp Data ONTAP 7-Mode device:

| Communication Direction | Protocol        | Ports                                   | Description |
|-------------------------|-----------------|-----------------------------------------|-------------|
| FAM to NetApp*          | HTTP (optional) | 80                                      | ONTAPI      |
| FAM to NetApp*          | HTTP (optional) | 443                                     | ONTAPI      |
| FAM to NetApp           | TCP             | 135, 139<br>Dynamic Range (49152-65535) | RPC         |
| FAM to NetApp           | TCP             | 445                                     | SMB         |
| FAM to NetApp           | UDP             | 137, 138                                | RPC         |
| NetApp to FAM           | TCP             | 135, 139<br>Dynamic Range (49152-65535) | RPC         |
| NetApp to FAM           | TCP             | 445                                     | SMB         |

| Communication Direction | Protocol | Ports    | Description |
|-------------------------|----------|----------|-------------|
| NetApp to FAM           | UDP      | 137, 138 | RPC         |

\*Only required if using the FPolicy Configuration and FPolicy Enable and Connect options within the File Activity Monitor.

#### EMC Firewall Rules

The following firewall settings are required for communication between FAM and the EMC Celerra, Dell EMC Unity, or EMC Isilon device:

| Communication Direction                      | Protocol | Ports             | Description       |
|----------------------------------------------|----------|-------------------|-------------------|
| EMC Isilon Device to CEE Server              | TCP      | TCP 12228         | CEE Communication |
| EMC Device (other than Isilon) to CEE Server | TCP      | RPC Dynamic Range | CEE Communication |

#### Hitachi Firewall Rules

The following firewall settings are required for communication between FAM and the Hitachi device:

| Communication Direction | Protocol | Ports | Description |
|-------------------------|----------|-------|-------------|
| Unidirectional          | TCP      | 445   | SMB         |

## SharePoint Permissions

- The provided domain user must be a local admin on the SharePoint application server.
- Auditing settings must be enabled on SharePoint.

## Installation

Use these instructions to install the File Activity Monitor (FAM) on your NAS or SharePoint environment.

### Before you begin

- Review the monitoring permissions: [Monitoring Permissions](#).
- For detailed platform prerequisites and support, see [Supported platforms for file activity monitoring](#).
- Prerequisite for EMC devices: To monitor an EMC device, the EMC Common Event Enabler (CEE) must be installed on the Windows proxy server where FAM is installed.

### Procedure

- To monitor a NAS device, install FAM on a Windows server that can access the NAS device through the network. To monitor SharePoint, install FAM directly on the SharePoint server or SharePoint server farm.  
Note: No other Guardium products must be installed on this server.
- Download the FAM for NAS or FAM for SharePoint package from [Fix Central](#) to the server and extract this file.
- From the FAM package installer directory and run the executable file **setup.exe** in the installer directory.
- Follow the prompts in the wizard to complete the installation.
  - In the Network Addresses screen, enter a list of Guardium hostnames or IP addresses. If there is a failover, the FAM agent connects to the next appliance on the list.  
Note:  
For NAS, the default installation directory is C:\Program Files\IBM\FAMforNAS  
For SharePoint, the default installation directory is C:\Program Files\IBM\FAMforSP

## Configuration

After installing, configure the File Activity Monitor (FAM) to begin monitoring your NAS or SharePoint environment.

Use the Policy builder for Files to configure monitoring for SharePoint and NAS devices. For more information, see [File activity policies for network-attached storage \(NAS\) and SharePoint](#)

FAM supports multiple services that are pointed to the same monitoring host. You can include multiple entries in the FAM configuration utility that point to different Guardium® appliances, have different local IP addresses, and include different policies. This feature provides the flexibility to create different rules for the same monitored host. You can monitor different parts of a share or site collection in the monitored host and report to different collectors.

## Viewing Results

To view file activity on your NAS device, use the NAS File Activities report. For SharePoint, use the SharePoint File Activities report.

### Procedure

- Click My Dashboards > Create New Dashboard to open a new dashboard.
- Click Add Report to display a list of available reports. The Add a Report dialog shows a list of all reports that meet your criteria. You can browse the list of reports or type a string in the Filter field. The list of reports is updated as you type.
- File activity on NAS devices can be viewed through the NAS File Activities report and file activity on SharePoint can be viewed through the SharePoint File Activities report. Click the report to add it to your dashboard.

## Results

In order to view results, create and install a custom policy. The default installed policy is "Ignore Data Activity for Unknown Connections [template]", which ignores all traffic. For more information on how to create a policy, see [Creating and installing a policy and policy rules](#).

## Uninstallation

Uninstall the File Activity Monitor (FAM) for network-attached storage (NAS) devices or SharePoint by using the Windows Control Panel.

Note: If cmd.exe is open during uninstallation and the FAM for SharePoint folder is the current directory, then the folder is not removed. Close cmd.exe and delete the FAM for SharePoint folder manually. The folder is deleted automatically when the system restarts.

## How to use PCI/DSS Accelerator to implement PCI compliance

Configure IBM® Guardium®'s PCI/DSS Accelerator and create a series of policies and reports, in order to meet PCI/DSS requirements.

PCI/DSS (Payment Card Industry/ Data Security Standard) is a set of technical and operational requirements designed to protect cardholder data.

Value-added: Give customers a whole view of PCI/DSS and provide predefined policies and reports to save configuration time.

Follow these steps:

1. Configure PCI role.
2. Configure reports and policies that follow the requirements.

### Configure PCI role

1. Login via the Guardium GUI page using the "accessmgr" user account. Select a user (in this case, user1), and click on Roles.

The screenshot shows a table titled 'User Browser' with columns: Username, First Name, Last Name, Email, and Actions. There are three rows: 'accessmgr' (First Name: accessmgr, Last Name: accessmgr, Email: user@pci.com, Actions: Edit, Roles, Change Layout), 'admin' (First Name: admin, Last Name: admin, Email: user@pci.com, Actions: Edit, Roles, Change Layout), and 'user1' (First Name: user, Last Name: pci, Email: user@pci.com, Actions: Edit, Roles, Change Layout, Delete). The 'Edit' and 'Roles' buttons are highlighted in red.

2. In the user role form, check PCI, and then save the assignment.

The screenshot shows the 'User Role Form' for user 'user1'. The title is 'Roles for user pci'. A table lists roles with checkboxes for assignment. The 'pci' role has a checked checkbox and is highlighted with a red border. Other roles listed include accessmgr, admin, appdev, audit, cas, cli, datasec-exempt, dba, diag, infosec, inv, netadm, optim-audit, review-only, and user. At the bottom are 'Save' and 'Back' buttons.

## Implement PCI accelerator

Log on using "user1" and click Accelerators.



## Overview

1. Click PCI Accelerator for Compliance.
2. Click PCI Data Security Standard.

### PCI Accelerator for Compliance

The PCI Data Security Standard consists of twelve basic requirements. Several of the requirements are focused on protecting physical infrastructure (for instance, Requirement 1: Install and maintain a firewall configuration to protect data) or implementing procedural best practices (for instance, Requirement 5: Use and regularly update anti-virus software). However, an additional, heavy emphasis is placed on real-time monitoring and tracking of access to cardholder data and continuous assessment of database security health status (for instance, Requirement 10: Track and monitor all access to network resources and cardholder data).

The PCI Accelerator simplifies organizational processes needed to support these monitoring and tracking mandates and to allow for cardholder data security. The Accelerator report templates can be customized to directly reflect specific organizational and regulatory requirements. You can access these templates using the tabs provided:

- PCI Data Security Standard overview
- Plan and Organize
- PCI Req. 10: Track and Monitor Access
- PCI Req. 11: Regularly Test and Validate
- PCI Policy Violations Monitoring

Other tools in the Guardium family of solutions available to assist in meeting regulations include the following:

- **Cardholder Database Access Map** - A graphical map of access between cardholder database access clients and servers. This map provides an at-a-glance view of activities by access type, content, and frequency. To open the Access Map builder and viewer, select View > Access Map > Access Map builder.
- **PCI Compliance Security Assessments** - A detailed view of database access security health used to automate the compliance processes with continuous real-time snapshots customized for user defined tests, weights, and assessments. The security assessment acts as a "report card" to help track progress on addressing database vulnerabilities. To create a security assessment, select Assess/Harden > Vulnerability Assessment > Assessment builder.
- **Full Audit Trail** - The non-intrusive generation of a full audit trail for data usage and modifications required by regulatory compliance. This capability is located under the Monitor/Audit tab.
- **Automated Scheduling** - Automated scheduling of PCI work flows, audit tasks, and distribution of information to responsible parties across the organization. This functionality is located under the Comply tab.



### PCI Data Security Standard

The Payment Card Industry (PCI) Data Security Standard offers a single approach to safeguarding sensitive data for all credit card brands. This standard is the result of collaboration between Visa and MasterCard, with the objective of creating common industry security requirements. Other card companies operating in the U.S. have also endorsed the PCI Data Security Standard within their respective programs.

The PCI Data Security Standard delivers a framework of tools and measurements needed to protect against cardholder data exposure and compromise across the entire payment industry. It applies to all members, merchants, and service providers that store, process, or transmit cardholder data utilizing any payment channels, including retail (brick-and-mortar), mail/telephone order, and e-commerce.

### PCI Compliance Validation

Separate and distinct from the mandate to comply with PCI requirements is the validation of compliance. The validation process is a fundamental and critical function that identifies and corrects vulnerabilities, and protects customers by ensuring that appropriate levels of cardholder information security are maintained. Card vendors have prioritized and defined levels of PCI compliance validation based on the volume of transactions, the potential risk, and exposure introduced into the systems by merchants and service providers. These include:

- Internal control
- Ongoing assessment (i.e., governance, measurement, and recordkeeping)
- Disclosure (i.e., investigation, reporting, and certification)

## Plan and Organize

### Plan and Organize

Click the Overview for an introduction of how the predefined reports follow the compliance.

1. Cardholder Server IPs List: Cardholder information database server list. According to the company's actual situation, set the PCI Authorized Server IPs group information, which specifies the database server that stores cardholder information.
2. Cardholders Databases: Cardholder information database. Set the PCI Cardholder DB: designated group information, which is stored in the database's cardholder information.
3. Cardholder Objects: Cardholder information object. This needs to set the PCI Cardholder Sensitive objects.
4. DB Clients to Servers Map: Client/server mapping and PCI Authorized Server IPs set group information, which specifies the database servers storing cardholder information. Query can be used to find client access to the cardholder database.
5. Active DB Users: Administrator in addition to categories of users, which visited the cardholder database. Set the "PCI Authorized Server IPs" and "PCI Admin Users".
6. Cardholder DB Administration: Cardholder database management operations. Set the PCI Authorized Server IPs and Admin Users.
7. Authorized Source Programs: Credit program access. Set the PCI Authorized Server IPs, PCI Authorized Source Programs. Procedure for recording Credit Cardholder database access.
8. Unauthorized Application Access: Non-credit program access. Set the PCI Authorized Server IPs, PCI Authorized Source Programs. Records of credit program for the cardholder database access.
9. 8.5.8 Shared Accounts: PCI eighth requirements to have each person having computer access to be assigned a unique ID. Set PCI Authorized Server IPs to count the number of times the same database username is trying to access from the cardholder database IP.

In the statements, click to view a report form, and then determine what specific group content needs to be filled in.

Here is the actual name of the group:

Navigate to Setup > Tools and Views > Group Builder, and in the Modify Existing Groups selection, select the group name.

Click Modify (the pencil icon) and go to Manage Members for Selected Group page. Add new members.

The group can also be filled through a customized query.

#### PCI Req. 10 Track & Monitor

Click the Overview for an introduction of how the Guardium monitor and predefined reports follow the compliance.

1. 10.2 and 10.3 Automation - Use the online help Protect help book and Comply Help book to automate this section.
2. 10.2.1 Data Access - PCI Access to cardholder data, Set the PCI Authorized Server IPs and PCI Admin Users.
3. 10.2.2 Admin Activity - PCI Activity by Admin. user. Set the PCI Authorized Server IPs and PCI Admin Users.
4. 10.2.3 Audit Trail Access - To follow this section completely, at least four kinds of reports must be defined: Logins to SQLGuard; User activity audit trails on Guardium server; Scheduled job exceptions; and, User to-to lists. Navigate to investigate > Query-Report Builder to create reports as you need.
5. 10.2.4 Invalid Access - PCI - Invalid Login Access Attempts: record the login failed try in the database. PCI - Unauthorized Application access: record the database access not defined in PCI Authorized Source Programs.
6. These three sections can also use the Monitor and Audit Help Book in the embedded online help - 10.2.6 Initialization Log, 10.5 Secure audit trails, and 10.6 Access Auditing.

#### PCI Req. 11 Ongoing Validation

Click Overview for a discussion on the importance of vulnerabilities assessment. Click Harden > Assessment Builder to build an assessment process.

#### PCI Policy Monitoring

Click Overview to introduce the Policy.

1. To show your current policy installations, navigate to Setup > Tools and Views > Policy Installation and choose a suitable policy for installation.

The screenshot displays two windows side-by-side. The left window is titled 'Policy Violation Count' and shows a large blue '0' indicating no violations. The right window is titled 'Currently Installed Policies' and lists one policy entry: 'Policy\_for\_uninstall\_Rule\_0002' with a date of '2016-07-15 07:15:07'.

2. Policy Violations - Records of violation operations.

## Workflow Builder

Use the Workflow Builder to define customized workflows (steps, transitions, and actions) that you can use with audit processes.

For additional information, see [Building audit processes](#). Follow these steps to:

- Define the workflow steps (Event Status)
- Define the flow of transit from one step to another (Actions)
- Define which actions require sign-off
- Assign roles to each status, to define the users permitted to view each status

Relevant Terms for this feature

Event Type - Custom workflow

Event Status - State/status of the workflow.

Event Action - Action/Transition

Note: Workflow Builder is an optional component enabled by product key.

## Create a Workflow Process

1. With an Admin account, open the Workflow Builder by navigating to Comply > Tools and Views > Workflow Builder. With a User account that has DataPrivacy privileges, open the Workflow Builder by navigating to Accelerators > Data Privacy > Track & Monitor > Audit Trail and Workflow Automation.
2. At the first screen (Event Type), click Event Status to go to the Event Status configuration.
3. Click Add Event Status to define a new Event Status. A multiple of Event Status are expected. Fill in the status description and place a check mark in the Is Final check box if the task is a final task in the workflow.
4. Click Event Type and then click Add on Add Event Type Definition to define a new Event Type.
5. Fill in the description and designate the first task in the workflow.
6. Then choose all the Allowed Status for the workflow from the Available Status list, by highlighting the Status item and clicking on the > button between the Available Status List and Allowed Status List.
7. When done, click the Save button. Note: the Save button (or Cancel button) only apply to changes made to name, default event or available events.
8. Go to the Defined Event Actions section of the Event Type menu screen. Defined Event Actions involves designating the separate Event Actions of the workflow.
9. Click the New button.
10. Fill in the Event Action Description and designate Prior status, Next status and if Sign-off of this event action is required. Click the Apply button.
11. Repeat Steps 9 and 10 until all event actions are described and designated.
12. Go to the Roles section of the Event Type menu screen. Roles involve defining who can see the event when it is in a particular Event Action. For example, who can see events that are "Under Review" and who can see events that are "Approved".
13. Select the Event Type Status and click the Roles button.
14. In the Assign Security Roles panel, mark all of the roles you want to assign (you will only see the roles that have been assigned to your account). Click Apply to save security role choices. Click the Back button.
15. Repeat steps 13 through 14 until all event type status have had roles defined.
16. The configuration effort from Workflow Builder is done.
17. Open the Audit Process Builder by navigating to Comply > Tools and Views > Audit Process Builder to schedule the workflow and build and show workflow reports. See the Audit Process Builder steps under Define a Report Task.

There is a usage scenario, Workflow Builder Workflow Example in the Appendices.

Note: If the task type in Audit Process Builder is Classification Process, then Workflow Builder can not create customized workflows.

Warning Note: When a workflow event is created, every status used by that event can be assigned a role (meaning that events can only be seen by this role when in this status). When an event is assigned to an audit process, it is important that every role that is assigned to a status of this event have a receiver on this audit process.

Otherwise, it is possible that an audit result row can be put into a status where none of its receivers are able to see this row or change its status.

If an audit row becomes inaccessible, the admin user (who is able to see all events, regardless of their roles) would be able to see the row and change its status. However, if data level security is on, the admin user may not be able to see this row. The admin user would need to either turn data level security off (from Global Profile) or have the dataset\_exempt role. It is important to configure the audit process so that all roles who must act on an event associated with this audit process are receivers of this audit process.

Note: Deletion of a event status is permitted only if the status is not in the first or final status of any events, and if it not used by any action. The validation will provide a list of events/actions that prevent the status from being deleted.

## Add Default Events only to limited number of records

---

When running an Audit Process report task, the results of this process task are saved in the table, REPORT\_RESULT\_DATA\_ROW. This table will have a row for every row of the report. If this report task also has a default event assigned to it, a row is added to the table, TASK\_RESULT\_ADDITIONAL\_INFO, for every row of the report. This may lead to a disk space issue only if default events are used for large results. Create events only on task results with a limited number of records, otherwise users will never be able to manage the large number of records. If default events are used in the intended limited manner, there will not be any disk space issues nor any usability issues, since it is not easy to close thousands of events.

- [\*\*How to create Customized Workflows\*\*](#)

Define customized workflows made up of specific customer steps, transitions and actions to be further used in an audit process.

- [\*\*How to use Customized Workflows\*\*](#)

Define an audit process that follows the customer's customized workflow practices. Bring the customer's specific auditing processes and practices into the Guardium® solution.

- [\*\*Opening Workflow Process Results\*\*](#)

Use View to see the Workflow Process Results

---

## How to create Customized Workflows

Define customized workflows made up of specific customer steps, transitions and actions to be further used in an audit process.

### About this task

---

Define and manage workflow based on customer's specific practices.

See Workflow Builder for an overview of this component.

#### Prerequisites

- See How to create an Audit Workflow. For additional information, see Compliance Workflow Automation.
- After creating this customized workflow, See How to combine Customized Workflow with Audit Workflow.

### Procedure

---

1. Open the Workflow Builder by navigating to Comply > Tools and Views > Workflow Builder.
2. At the first screen (Event Type), click the Event Status button to go to the Event Status configuration.
3. Click on Add Event Status to define a new Event Status. A multiple of Event Status are expected. Fill in the status description and place a check mark in the Is Final check box if the task is a final task in the workflow. When done, go to the next step.

An example of a simple three-step workflow is: Open to Review state to Approve or Not Approved. Each step of the workflow is a separate Defined Task Event Status.

The workflow tasks of the example are: Open, Review state, Approve after review, or Not approved. Also, if the task is the final task in a workflow, place a check mark in the Is Final column. Examples of a final task in the example are Approved or Not Approved.

View Quick Start Monitor/Audit Discover Assess/Harden Comply  Protect

Compliance Automation     

### Event Type

**Existing Task Event Types**

| Event Type    | First Status | Allowed Status                                         |
|---------------|--------------|--------------------------------------------------------|
| * My workflow | Open         | Approve after review, Not approved, Open, Review State |

**Edit Event Type Definition My workflow**

Description: My workflow

First Status: Open

**Allowed Status**

Available Status:

Allowed Status: Approve after review (Final), Not approved (Final), Open, Review State

**Defined Event Actions**

|                                                                                                                                                                                                                                                       | Event Action Description | Prior Status | Next Status          | Sign-off                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------|----------------------|-------------------------------------|
|    | Under Review             | Open         | Review State         | <input type="checkbox"/>            |
|    | Approved                 | Review State | Approve after review | <input checked="" type="checkbox"/> |
|    | Not approved             | Review State | Not approved         | <input checked="" type="checkbox"/> |

**New...**

**Roles**

Roles have been assigned to this event type with status Approve after review

Roles have been assigned to this event type with status Not approved

Roles have been assigned to this event type with status Open

Roles have been assigned to this event type with status Review State

**Cancel** **Save**

**New Event Type** **Event Status**

4. Click on the Event Type button and then click on the Add button of Add Event Type Definition to define a new Event Type.
5. Fill in the description and designate the first task in the workflow.
6. Then choose all the Allowed Status for the workflow from the Available Status list, by highlighting the Status item and clicking on the > button between the Available Status List and Allowed Status List.
7. When done, click the Save button.
8. Go to the Defined Event Actions section of the Event Type menu screen. Defined Event Actions involves designating the separate Event Actions of the workflow.
9. Click the New button.
- From the simple three-step workflow example, an Event Action of Under Review has a prior status of Open and a next Status of Review State. The Event Action of Approved follows Under Review with a prior status of Review State and next status of Approve after review. Or the Event Action of Not approved has a prior status of Review State and a next status of Not Approved. There is also a signoff capability for designated reviewers per Event Action (continuous or sequential). See the previous screen shot.
10. Fill in the Event Action Description and designate Prior status, Next status and if Sign-off of this event action is required. Click the Apply button.
11. Repeat Steps 9 and 10 until all event actions are described and designated.
12. Go to the Roles section of the Event Type menu screen. Roles involve defining who can see the event when it is in a particular Event Action. For example, who can see events that are "Under Review" and who can see events that are "Approved".
13. Select the Event Type Status and click the Roles button.
14. In the Assign Security Roles panel, mark all of the roles you want to assign (you will only see the roles that have been assigned to your account). Click Apply to save security role choices. Click the Back button.
15. Repeat steps 13 through 14 until all event type status have had roles defined.
16. The configuration effort from Workflow Builder is done.
17. Open the Audit Process Builder by navigating to Comply>Tools and Views>Audit Process Builder to schedule the workflow and build and show workflow reports. See the Audit Process Builder steps under Define a Report Task.

## How to use Customized Workflows

Define an audit process that follows the customer's customized workflow practices. Bring the customer's specific auditing processes and practices into the Guardium® solution.

### About this task

## Customized Workflows within the Guardium Audit Workflow process

The formal sequence of event types created in Workflow Builder is managed by clicking on the Event and Additional Column button in the Audit Tasks window. This button will appear after an audit task has been created and saved. This additional button will not appear until the audit task is saved.

### Prerequisites

- See How to create Customized Workflows. For additional information, see Workflow Builder.
- See How to create an Audit Workflow. For additional information, see Compliance Workflow Automation.
- Define an audit process that follows the customer's customized workflow practices by following the additional steps.

## Procedure

1. Configure these workflow activities when Adding An Audit Task.
2. Create and save an Audit Task. After saving, an additional button, Events and Additional Columns, will appear.
3. Click this additional button.

| Column Name   | Mandatory                           | Type   | Size | Group |
|---------------|-------------------------------------|--------|------|-------|
| Company Code  | <input checked="" type="checkbox"/> | String | 50   |       |
| Business Unit | <input checked="" type="checkbox"/> | String | 50   |       |
|               | <input type="checkbox"/>            | String | 50   |       |

[Close this window](#)

4. At the next screen, place a checkmark in the box for Event & Sign-off. The workflow created in Workflow Builder will appear as a choice in Event & Sign-off.
5. Highlight this choice. Save your selection.
6. If additional information (such as company codes, business unit labels, etc.) is needed as part of the workflow report, add this information in the Additional Column section of the screen and then click Apply (save). When done, close this window.
7. Apply (save) your Audit Task. Apply (save) the entire Audit Process Definition. Click on the Run Once Now to create the report. Click on View to see the report.
8. Click on the Run Once Now to create the report. Click on View to see the report.

| User Name | Login Succeeded  | Login Date And Time | Logout Date And Time | Host Name | Remote Address | # | Company Code | Business Unit | Event/Status            | Sign | By                                |
|-----------|------------------|---------------------|----------------------|-----------|----------------|---|--------------|---------------|-------------------------|------|-----------------------------------|
| admin     | Login Succeeded  | 2009-10-22 07:23:18 | 2009-10-22 08:07:44  | vx29      | 192.168.1.115  | 1 |              |               | Company A workflow/Open |      | Default Event 2009-10-23 08:25:33 |
| admin     | Login Succeeded  | 2009-10-22 07:49:07 |                      |           | 192.168.1.134  | 1 |              |               | Company A workflow/Open |      | Default Event 2009-10-23 08:25:33 |
| admin     | Login Succeeded  | 2009-10-22 08:14:35 |                      |           | 192.168.1.115  | 1 |              |               | Company A workflow/Open |      | Default Event 2009-10-23 08:25:33 |
| admin     | Login Succeeded  | 2009-10-22 08:27:12 |                      |           | 192.168.1.111  | 1 |              |               | Company A workflow/Open |      | Default Event 2009-10-23 08:25:33 |
| admin     | Login Succeeded  | 2009-10-22 09:32:17 |                      |           | 192.168.168.2  | 1 |              |               | Company A workflow/Open |      | Default Event 2009-10-23 08:25:33 |
| admin     | Login Succeeded  | 2009-10-22 10:11:16 |                      |           | 192.168.168.2  | 1 |              |               | Company A workflow/Open |      | Default Event 2009-10-23 08:25:33 |
| admin     | Login Succeeded  | 2009-10-22 10:59:27 |                      |           | 192.168.1.115  | 1 |              |               | Company A workflow/Open |      | Default Event 2009-10-23 08:25:33 |
| admin     | Login Succeeded  | 2009-10-22 12:01:22 |                      |           | 192.168.1.115  | 1 |              |               | Company A workflow/Open |      | Default Event 2009-10-23 08:25:33 |
| admin     | Login Succeeded  | 2009-10-22 12:43:52 |                      |           | 192.168.168.2  | 1 |              |               | Company A workflow/Open |      | Default Event 2009-10-23 08:25:33 |
| admin     | Login Succeeded  | 2009-10-22 14:04:08 |                      |           | 192.168.168.2  | 1 |              |               | Company A workflow/Open |      | Default Event 2009-10-23 08:25:33 |
| admin     | Login Succeeded  | 2009-10-22 14:13:07 |                      |           | 192.168.168.2  | 1 |              |               | Company A workflow/Open |      | Default Event 2009-10-23 08:25:33 |
| admin     | Login Succeeded  | 2009-10-22 14:15:20 |                      |           | 192.168.168.2  | 1 |              |               | Company A workflow/Open |      | Default Event 2009-10-23 08:25:33 |
| admin     | Login Succeeded  | 2009-10-22 15:14:43 |                      |           | 192.168.1.111  | 1 |              |               | Company A workflow/Open |      | Default Event 2009-10-23 08:25:33 |
| admin     | Login Succeeded  | 2009-10-23 07:39:21 |                      |           | 192.168.1.115  | 1 |              |               | Company A workflow/Open |      | Default Event 2009-10-23 08:25:33 |
| billpa    | Password Expired | 2009-10-20 09:06:54 |                      |           | 192.168.1.115  | 1 |              |               | Company A workflow/Open |      | Default Event 2009-10-23 08:25:33 |
| billpa    | Login Succeeded  | 2009-10-20 09:06:54 |                      |           | 192.168.1.115  | 1 |              |               | Company A workflow/Open |      | Default Event 2009-10-23 08:25:33 |
| billpa    | Login Succeeded  | 2009-10-20 09:23:04 |                      |           | 192.168.1.115  | 1 |              |               | Company A workflow/Open |      | Default Event 2009-10-23 08:25:33 |

This Event and Additional Column button appears in all audit tasks.

Note: If data level security at the observed data level has been enabled (see Global Profile settings), then audit process output will be filtered so users will see only the information of their databases.

Under the Report choices within Add an Audit Task are two procedural reports, Outstanding Events and Event Status Transition. Add these two reports to two new audit tasks to show details of all workflow events and transitions. These two reports will not be filtered (observed data level security filtering will not be applied). These two reports are available by default in the list of reports only to admin user and users with the admin role.

# Opening Workflow Process Results

Use View to see the Workflow Process Results

Do one of the following:

- Open your Workflow Automation To-do List (see Audit Process To-Do List) and click View for the results set you want to view or sign.
- If you have received an e-mail notification containing hypertext links to your To-Do List or the results, click one of those links to open your To-Do List or the results directly from the e-mail. You must have access to the Guardium® system at the location from which you are accessing your e-mail (or these links will not work). If you are not logged in, you will be prompted to log in to the Guardium system.

Note: When you register a new managed unit to a central manager, you might be unable to view audit results. The application does not show results that have a timestamp before the managed unit was registered to the central manager. The timestamp of the registration uses the central manager time, and the timestamp of the audit result uses the managed node time. So, if the central manager time is ahead of the managed unit time, results generated on the managed unit are not visible until the managed unit time passes the time of registration. This should happen in no more than 24 hours, possibly less depending on the locations of the two machines. You should be able to view the results of audit processes on the managed unit within 24 hours of registration.

## Reports

Data protection requires monitoring of data and file activity. Guardium gathers a large amount of data about your database environment, and about your Guardium system. You can view this data in reports.

Guardium provides sophisticated reporting tools that includes many predefined reports. However, you may want to build your own custom report or to modify an existing report.

Each report presents information that is defined by the report's unique query. The query defines what information is gathered, and how it is displayed in the report. Queries are also used to gather information for other purposes. For example, a group can be populated from the results of a query.

You can use dashboards to group reports for display. You can add custom reports and predefined reports to a dashboard, and to My Custom Reports.

## Limitations

- PDFs generated manually or using an audit process are limited to 5,000 rows. Manually exported CSV files are limited to 30,000 rows (this default is configurable using the `store csv_max_size` CLI command). Any number of rows can be exported to CSV when using an audit process. For more information, see [Building audit processes](#) and [Exporting a report](#).
- Group builder and Alias builder. When importing group members from Members tab, Import From query using Run Once Now, the maximum number of imported members is 5,000 rows. This is not configurable. For more information, see [Populating groups](#) and [Define Aliases using a Query](#).
- Group builder and Alias builder. When importing group members from Members tab, Import From query using a schedule, the maximum number of imported members is 20,000 rows by default. You can configure this limit using the CLI command `show/store populate_from_query_maxrecs`. For more information, see [Populating groups](#) and [Define Aliases using a Query](#).
- **Predefined reports**  
Before creating custom reports from scratch, take advantage of the predefined Guardium reports.
- **Creating dashboards and adding reports**  
You can create one or more dashboards, add reports to them, and configure their appearance.
- **Opening the investigation dashboard, filtered for report entities**
- **Viewing reports**  
There are several ways to view a report, including your dashboard and UI search.
- **Using the Query-Report Builder**  
If the predefined reports do not meet your needs, create a query from scratch, or clone and modify an existing query.
- **Domains, Entities, and Attributes**  
Each domain contains a set of data stored in Guardium that relates to a specific purpose or function (data access, exceptions, policy violations, and so forth). The data is grouped by entities. An entity is a set of related attributes, and an attribute is basically a field value.
- **Custom Domains**  
Custom domains allow for user defined domains and can define any tables of data uploaded to your Guardium system.
- **Data Mart**  
Use data marts to extract data for subsequent use. Use datamarts for more efficient storage of frequently accessed data; for data that you want to preserve after its purge time; for exporting data from Guardium; and for creating distributed reports.
- **Distributed Report Builder**  
This central manager feature provides a way to automatically gather data from all or a subset of the Guardium managed units that are associated with this particular central manager. Distributed reports are designed to provide a high-level view, to correlate data from across data sources, and to summarize views of the data. Continue to use aggregators for the row level data gathering across collectors.
- **Working with API calls and reports**
- **Working with external feeds**  
Use external feeds to send Guardium report data directly to an external database. Sending reporting data to an external database is useful in several scenarios, for example when combining or correlating Guardium data with non-Guardium data, when using Guardium data with external tools, or when machine-parsing records in especially large reports.
- **Creating reports for z/OS**  
Learn how to create Guardium reports for z/OS data sources by customizing built-in reports and example queries.

## Predefined reports

Before creating custom reports from scratch, take advantage of the predefined Guardium reports.

Get the information that you seek faster, by accessing predefined reports available from the Guardium application. These predefined reports can be cloned and customized to the needs of the user.

Using the Guardium predefined reports is a best practice recommendation, enabling organizations to quickly and easily identify security risks, such as inappropriately exposed objects, users with excessive rights, and unauthorized administrative actions. Examples of the many predefined reports include: accounts with system privileges; all system and administrator privileges, which are shown by user and role; object privileges by user; and all objects with PUBLIC access.

The parameters (columns) display can be edited using Customize in any report screen.

Use the search function of help to go to the specific report directly. Use quotation marks around words or phrases to precisely define search terms.

## Use cases for predefined reports

---

Database administrator

- SQL Errors - An increase in SQL errors may indicate a SQL injection attack.
- DDL (verify schema changes) - This report displays the client IP from which the DDL was requested, the main SQL verb (a specific DDL command), and the total objects accessed for that record.
- Failed logins - This report indicates attempts to access the database with expired login credentials.

Information security officer

- Failed logins - People with proper credentials trying to access the database.
- Terminated users - Terminated users trying to access the database.
- Policy violations - Users and issues that violate security policies.

Auditors

- Compliance reports - PCI, SOX, Data Privacy
- Compliance workflow - Shows evidence of signoffs and procedures.

- **Predefined admin reports**

This section provides a short description of predefined reports for the admin user.

- **Predefined user reports**

This section provides a short description of all predefined reports for users with default user access.

- **Predefined common reports**

This section provides a short description of all predefined reports available for users with either default user access rights or default admin access rights.

---

## Predefined admin reports

This section provides a short description of predefined reports for the admin user.

Note: If data level security at the observed data level is enabled (see [Data level security filtering](#)), then the audit process output is filtered so users see only the information about their databases.

**Enterprise reports with custom tables:** If for any reason, the central manager did not receive data from a managed unit for the custom table in an enterprise report in the last 24 hours, the Guardium® UI banner displays the message:

Central manager experienced failure getting data from collector. Central manager experienced error in the last 24 hours uploading data.

Click the report name to open the Scheduled Jobs Exceptions report and view details of the managed units that had exceptions.

The predefined admin reports are listed in alphabetical order.

## Active Risk Spotter - Risky Users Scores

---

This report details the current risky users, including the server IP, the overall risk score, and scores for all of the risk indicators.

## Active S-TAPs changed

---

This alert only runs on Central Manager systems. S-TAP Host, S-TAP version, S-TAP changed, timestamp and count are shown.

| Domain                   | Based on Query        | Main Entity   |
|--------------------------|-----------------------|---------------|
| Internal - not available | Active S-TAPs changed | Not available |
| Run-Time Parameter       | Operator              | Default Value |
| Period From              | none                  | none          |

## Admin User Logins

---

Summary of logins to the database using a database user name defined in the Admin Users group. The report displays the client IP address from which the user with administrative privileges logged into the database, database user name, source program, session start date and time, and session total for that record.

| Domain             | Based on Query    | Main Entity   |
|--------------------|-------------------|---------------|
| Access             | Admin Users Login | Session       |
| Run-Time Parameter | Operator          | Default Value |
| Period From        | >=                | NOW -1 DAY    |
| Period To          | <=                | NOW           |

## Aggregation/Archive Log

This report lists Guardium aggregation activity by Activity Type. Each row of the report contains the Activity Type, Start Time, File Name, Status, Comment, Guardium Host Name, Records Purged, Period Start, Period End, and count of log records for the row. You can limit the output by setting the Guardium Host Name run-time parameter, which is set to % by default (to select all servers). The Records Purged column contains a count of records purged only when the activity type is Purge.

| Domain                    | Based on Query          | Main Entity     |
|---------------------------|-------------------------|-----------------|
| Aggregation/Export/Import | Aggregation/Archive Log | Agg/Archive Log |
| Run-Time Parameter        | Operator                | Default Value   |
| Period From               | >=                      | NOW -1 WEEK     |
| Period To                 | <=                      | NOW             |
| Guardium Host Name        | LIKE                    | %               |

## 12.1 and later Aggregator Global Collector ID

This report maps the collector ID and collector name to the aggregator.

| Domain                         | Based on Query                 | Main Entity                    |
|--------------------------------|--------------------------------|--------------------------------|
| Aggregator Global Collector ID | Aggregator Global Collector ID | Aggregator Global Collector ID |
| Run-Time Parameter             | Operator                       | Default Value                  |
| Period From                    | >=                             | NOW -3 HOUR                    |
| Period To                      | <=                             | NOW                            |
| Show Aliases                   | Radio buttons                  | Default                        |
| Remote Data Source             | Drop-down menu                 |                                |
| Refresh Rate                   | Drop-down menu                 | 0                              |

## All Guardium Applications - Roles

This menu pane displays two reports: All Roles - Application Access - and All Roles - User.

### All Roles - Application Access

For each role, this report lists the number of applications to which it is assigned. To list the applications to which a role is assigned, click on the role and drill down to the Record Details report.

| Domain                   | Based on Query                 | Main Entity    |
|--------------------------|--------------------------------|----------------|
| Internal - not available | All Roles - Application Access | Not available  |
| Run-Time Parameter       | Operator                       | Default Value  |
| Period From              | >=                             | NOW -100 MONTH |
| Period To                | <=                             | NOW            |

### All Roles - User

For each role, this report lists the number of users to which it is assigned. To list the users to which a role is assigned, click on the role and drill down to the Record Details report.

| Domain                   | Based on Query | Main Entity    |
|--------------------------|----------------|----------------|
| Internal - not available | Role - User    | Not available  |
| Run-Time Parameter       | Operator       | Default Value  |
| Period From              | >=             | NOW -100 MONTH |
| Period To                | <=             | NOW            |

## Analytic Outlier Details

| Domain                    | Based on Query            | Main Entity               |
|---------------------------|---------------------------|---------------------------|
| Analytic Outliers Details | Analytic Outliers Details | Analytic Outliers Details |
| Run-Time Parameter        | Operator                  | Default Value             |
| Period From               | >=                        | NOW -3 HOUR               |
| Period To                 | <=                        | NOW                       |
| DB User name              | LIKE                      | %                         |
| DB Name                   | LIKE                      | %                         |
| Source program            | LIKE                      | %                         |
| Object                    | LIKE                      | %                         |
| Verb                      | LIKE                      | %                         |
| Client hostname           | LIKE                      | %                         |
| OS user                   | LIKE                      | %                         |

## Analytic Outlier Details List - enhanced

| Domain                    | Based on Query            | Main Entity               |
|---------------------------|---------------------------|---------------------------|
| Analytic Outliers Details | Analytic Outliers Details | Analytic Outliers Details |
| Run-Time Parameter        | Operator                  | Default Value             |

| Run-Time Parameter | Operator | Default Value |
|--------------------|----------|---------------|
| Period From        | >=       | NOW -3 HOUR   |
| Period To          | <=       | NOW           |
| DB User name       | LIKE     | %             |
| DB Name            | LIKE     | %             |
| Source program     | LIKE     | %             |
| Object             | LIKE     | %             |
| Verb               | LIKE     | %             |
| Client hostname    | LIKE     | %             |
| OS user            | LIKE     | %             |

## Analytic Outlier Summary

| Domain                    | Based on Query            | Main Entity               |
|---------------------------|---------------------------|---------------------------|
| Analytic Outliers Details | Analytic Outliers Details | Analytic Outliers Details |
| Run-Time Parameter        | Operator                  | Default Value             |
| Period From               | >=                        | NOW -3 HOUR               |
| Period To                 | <=                        | NOW                       |
| Server IP                 | LIKE                      | %                         |
| DB User name              | LIKE                      | %                         |
| DB Name                   | LIKE                      | %                         |
| OS User                   | LIKE                      | %                         |

## Analytic Outlier Summary by Date - enhanced

| Domain                    | Based on Query            | Main Entity               |
|---------------------------|---------------------------|---------------------------|
| Analytic Outliers Details | Analytic Outliers Details | Analytic Outliers Details |
| Run-Time Parameter        | Operator                  | Default Value             |
| Period From               | >=                        | NOW -3 HOUR               |
| Period To                 | <=                        | NOW                       |
| Server IP                 | LIKE                      | %                         |
| DB User name              | LIKE                      | %                         |
| DB Name                   | LIKE                      | %                         |
| OS User                   | LIKE                      | %                         |

## Analytic Threat Case Details

This report presents details of an identified threat case. You need to enter the case ID and the datasource to view the report.

| Domain                  | Based on Query | Main Entity                      |
|-------------------------|----------------|----------------------------------|
| Eagle Eye               | Not available  | Symptom type                     |
| Run-Time Parameter      | Operator       | Default Value                    |
| Enter Value for Case Id |                | text field                       |
| Show Aliases            |                | Radio buttons (On, Off, Default) |
| Remote Data Source      |                | Drop-down menu                   |
| Refresh rate in seconds |                | 0                                |

## Appliance Settings

This report displays configuration settings from a Guardium system. Use the *appliance settings* report to quickly review and validate Guardium settings.

| Domain                   | Based on Query        | Main Entity                      |
|--------------------------|-----------------------|----------------------------------|
| Internal - not available | Active S-TAPs changed | Not available                    |
| Run-Time Parameter       | Operator              | Default Value                    |
| Show Aliases             |                       | Radio buttons (On, Off, Default) |
| Remote Data Source       |                       | Drop-down menu                   |

## Application Objects Summary

This report is a summary of every definition in the Guardium application. For instance, type Oracle in the ObjectNameLike space in the Run-Time Parameters page of Application Objects and find all the Object Types and Object Descriptions where Oracle is used.

Note: This report presents metadata and as such is not filtered through the Data Level Security mechanism. This metadata could include database related information such as Oracle SIDs.

| Domain              | Based on Query              | Main Entity         |
|---------------------|-----------------------------|---------------------|
| Application Objects | Application Objects Summary | Application Objects |
| Run-Time Parameter  | Operator                    | Default Value       |
| ObjectNameLike      | %                           | %                   |
| ObjectTypeLike      | %                           | %                   |

## Approved TAP clients

Only specific S-TAPs are permitted to connect to the Guardium application. This report shows which S-TAP is approved and the status of it.

| Domain                   | Based on Query       | Main Entity   |
|--------------------------|----------------------|---------------|
| Internal - not available | Approved TAP Clients | Not available |
| Run-Time Parameter       | Operator             | Default Value |
| Period From              | >=                   | NOW -1 DAY    |
| Period To                | <=                   | NOW           |

## Assessment Datasources

This report is a summary of datasources that are linked to a security assessment.

| Domain                   | Based on Query                                                               |               | Main Entity         |
|--------------------------|------------------------------------------------------------------------------|---------------|---------------------|
| Internal - not available | Assessment and the datasources (or datasource groups) used by the assessment |               | SECURITY_ASSESSMENT |
| Run-Time Parameter       | Operator                                                                     | Default Value |                     |
| Assessment               | LIKE                                                                         | %             |                     |
| Refresh rate in seconds  |                                                                              | 0             |                     |

## Assessment Roles Allowed

This report is a summary of the roles that are mapped to a security assessment.

| Domain                   | Based on Query                                     |               | Main Entity         |
|--------------------------|----------------------------------------------------|---------------|---------------------|
| Internal - not available | Assessment and the roles defined in the assessment |               | SECURITY_ASSESSMENT |
| Run-Time Parameter       | Operator                                           | Default Value |                     |
| Assessment               | LIKE                                               | %             |                     |
| Refresh rate in seconds  |                                                    | 0             |                     |

## Assessment Tests

This report lists the tests that are included in a security assessment.

| Domain                   | Based on Query                                                          |                                  | Main Entity         |
|--------------------------|-------------------------------------------------------------------------|----------------------------------|---------------------|
| Internal - not available | Assessment and the associated tests that are included in the assessment |                                  | SECURITY_ASSESSMENT |
| Run-Time Parameter       | Operator                                                                | Default Value                    |                     |
| Period From              | >=                                                                      | 2009-01-01 00:00:00              |                     |
| Period To                | <=                                                                      | NOW                              |                     |
| Assessment               | LIKE                                                                    | %                                |                     |
| Test Description         | LIKE                                                                    | %                                |                     |
| Assessment ID            | LIKE                                                                    | %                                |                     |
| Test ID                  | LIKE                                                                    | %                                |                     |
| Show Aliases             |                                                                         | Radio buttons (On, Off, Default) |                     |
| Remote Data Source       |                                                                         | Drop-down menu                   |                     |
| Refresh Rate (Seconds)   |                                                                         | 0                                |                     |

## Available VA Tests

Following reports are available as part of Available VA Tests

- Available VA Tests
- Available VA Tests - Detailed
- 12.1 and later Available VA Tests - CIS
- 12.1 and later Available VA Tests - STIG

The Available VA Tests report and Available VA Tests - Detailed report lists all the security assessment tests in the Guardium system where the reports are generated. The **Available VA Tests - Detailed** report is a more comprehensive version of the **Available VA Tests** report. The Available VA Tests - CIS and Available VA Tests - STIG reports provide ability to filter VA Available Tests report by CIS and STIG, respectively.

### Available VA Tests report

Use the following selections to configure the Available VA Tests report:

| Domain             | Based on Query     | Main Entity                      |
|--------------------|--------------------|----------------------------------|
| VA Tests           | Available VA tests | Assessment Tests                 |
| Run-Time Parameter | Operator           | Default Value                    |
| Test Type          | LIKE               | %                                |
| Category           | LIKE               | %                                |
| Datasource Type    | LIKE               | %                                |
| Severity           | LIKE               | %                                |
| Show Aliases       |                    | Radio buttons (On, Off, Default) |
| Remote Data Source |                    | Drop-down menu                   |

| Run-Time Parameter     | Operator | Default Value |
|------------------------|----------|---------------|
| Refresh Rate (Seconds) |          | 0             |

#### Available VA Tests - Detailed report

Use the following selections to configure the Available VA Tests - Detailed report:

| Domain                    | Based on Query           | Main Entity                      |
|---------------------------|--------------------------|----------------------------------|
| Internal - not available  | Internal - not available | Internal - not available         |
| Run-Time Parameter        | Operator                 | Default Value                    |
| Period From               | >=                       | 2009-01-01 00:00:00              |
| Period To                 | <=                       | NOW                              |
| Test ID                   | LIKE                     | %                                |
| Test Description          | LIKE                     | %                                |
| Audit Config Template ID  | LIKE                     | %                                |
| Datasource Type           | LIKE                     | %                                |
| Severity                  | LIKE                     | %                                |
| Category Name             | LIKE                     | %                                |
| Short Description         | LIKE                     | %                                |
| External Reference        | LIKE                     | %                                |
| Can Have Exceptions Group | LIKE                     | %                                |
| Show Aliases              |                          | Radio buttons (On, Off, Default) |
| Remote Data Source        |                          | Drop-down menu                   |
| Refresh Rate (Seconds)    |                          | 0                                |

#### 12.1 and later Available VA Tests - CIS

| Domain                           | Based on Query           | Main Entity                      |
|----------------------------------|--------------------------|----------------------------------|
| Internal - not available         | Internal - not available | Internal - not available         |
| Run-Time Parameter               | Operator                 | Default Value                    |
| Enter Value for Test ID          | LIKE                     | %                                |
| Enter Value for Data source Type | LIKE                     | %                                |
| Enter Value for Severity         | LIKE                     | %                                |
| Enter Value for the Test Type    | LIKE                     | %                                |
| Enter Value for Category         | LIKE                     | %                                |
| Show Aliases                     |                          | Radio buttons (On, Off, Default) |
| Remote Data Source               |                          | Drop-down menu                   |
| Refresh Rate                     |                          | 0                                |

#### 12.1 and later Available VA Tests - STIG

| Domain                           | Based on Query           | Main Entity                      |
|----------------------------------|--------------------------|----------------------------------|
| Internal - not available         | Internal - not available | Internal - not available         |
| Run-Time Parameter               | Operator                 | Default Value                    |
| Enter Value for Test ID          | LIKE                     | %                                |
| Enter Value for Data source Type | LIKE                     | %                                |
| Enter Value for Severity         | LIKE                     | %                                |
| Enter Value for the Test Type    | LIKE                     | %                                |
| Enter Value for Category         | LIKE                     | %                                |
| Show Aliases                     |                          | Radio buttons (On, Off, Default) |
| Remote Data Source               |                          | Drop-down menu                   |
| Refresh Rate                     |                          | 0                                |

## Audit Process Log

### Audit Process Log

This report shows a detailed activity log for all tasks including start and end times. This report is available for admin users. Audit tasks show start and end times, however the start and end of Security Assessments and Classifications (which go to a queue) is the same.

The Audit Process has been expanded to the signoff of specific rows beyond a user signing off on the entire audit process. Displays a list of what has been signed off and what is the status of specific rows.

Use this Audit Process Log to stop audit processes. Tasks can be stopped only if the tasks have not been run or are running. Any more tasks that have not started will not execute. Partial results will not be delivered. If tasks are complete, stopping the audit process will not stop the sending of the results. Stopping the audit process is done through a GrdAPI command, invoke api, from the Audit process Log report. For any user it only shows the line belonging to the user (but without all the details - just the tasks). Admin users get to see all the details and can stop anyone's runs. Users can only stop their own runs.

Stopping the audit process does not cancel queries running using a remote source. Neither will such online reports using a remote source.

Not supported for Privacy sets and External Feed. This means that if the Privacy set task was started or the External Feed has started - it will finish even if the process is stopped (as opposed to a query which will be killed).

Audit Process Log ID

Login Name

Run ID

Timestamp

Audit Process ID  
 Audit Process Description  
 Audit Task ID  
 Audit Task Description  
 Event Type  
 Detail  
 Count of Audit Process Log

## Available Patches

Displays a list of available patches. There are no run-time parameters. The reporting domain is system-only.

## Audit Job Task Security Assessment

Displays the definition of the audit process job and the task name that runs a security assessment.

| Domain                   | Based on Query           | Main Entity              |
|--------------------------|--------------------------|--------------------------|
| Internal - not available | Internal - not available | Internal - not available |
| Run-Time Parameter       | Operator                 | Default Value            |
| Process ID               | LIKE                     | %                        |
| Task ID                  | LIKE                     | %                        |
| Process Description      | LIKE                     | %                        |
| Task Description         | LIKE                     | %                        |
| Assessment ID            | LIKE                     | %                        |
| Assessment Description   | LIKE                     | %                        |
| Refresh Rate (Seconds)   |                          | 0                        |
| Run-Time Parameter       | Operator                 | Default Value            |
| Process ID               | LIKE                     | %                        |
| Task ID                  | LIKE                     | %                        |

## 12.1 and later Audit Process Task Details

Provides audit process information including the Audit process items, audit tasks and the record count for the audit tasks that belong to the audit process items. This report is useful for validating the data that is sent to SIEM and ensures the same number of records are sent in a file.

| Domain                   | Based on Query                 | Main Entity   |
|--------------------------|--------------------------------|---------------|
| Internal - not available | All Roles - Application Access | Not available |
| Run-Time Parameter       | Operator                       | Default Value |
| Period From              | >=                             | NOW - 3 HOURS |
| Period To                | <=                             | NOW           |
| Remote Data Source       | Drop-down menu                 | --            |
| Show Aliases             | Radio buttons                  | Default       |
| Refresh Rate (Seconds)   | Drop-down menu                 | 0             |

## Buffer Usage Monitor

Provides an extensive set of buffer usage statistics. For more information, see [BigData Intelligence Buff Usage Monitor domain](#).

| Domain             | Based on Query     | Main Entity                  |
|--------------------|--------------------|------------------------------|
| Buffer Usage       | Buff Usage Monitor | Sniffer Buffer Usage Monitor |
| Run-Time Parameter | Operator           | Default Value                |
| Period From        | >=                 | NOW -1 DAY                   |
| Period To          | <=                 | NOW                          |

## Cassandra DB Object privileges granted to grantee

Lists all the Cassandra DB Object privileges that are granted to users and roles.

| Domain                                            | Based on Query                                    | Main Entity                                       |
|---------------------------------------------------|---------------------------------------------------|---------------------------------------------------|
| Cassandra DB Object privileges granted to grantee | Cassandra DB Object privileges granted to grantee | Cassandra DB Object privileges granted to grantee |
| Run-Time Parameter                                | Operator                                          | Default Value                                     |
| Period From                                       | >=                                                | NOW -3 HOUR                                       |
| Period To                                         | <=                                                | NOW                                               |
| Enter Value for Role                              | LIKE                                              | %                                                 |
| Enter Value for Resource                          | LIKE                                              | %                                                 |
| Enter Value for Permission                        | LIKE                                              | %                                                 |
| Show Aliases                                      | Radio buttons                                     | Default                                           |

| Run-Time Parameter     | Operator       | Default Value |
|------------------------|----------------|---------------|
| Remote Data Source     | Drop-down menu |               |
| Refresh Rate (Seconds) | Drop-down menu | 0             |

## Cassandra Object privileges granted with grant option

Lists all the Cassandra users and roles with Object privileges that can be granted to another user.

| Domain                                                |                | Based on Query                                        | Main Entity                                           |
|-------------------------------------------------------|----------------|-------------------------------------------------------|-------------------------------------------------------|
| Cassandra Object privileges granted with grant option |                | Cassandra Object privileges granted with grant option | Cassandra Object privileges granted with grant option |
| Run-Time Parameter                                    | Operator       | Default Value                                         |                                                       |
| Period From                                           | >=             | NOW -3 HOUR                                           |                                                       |
| Period To                                             | <=             | NOW                                                   |                                                       |
| Enter Value for Role                                  | LIKE           | %                                                     |                                                       |
| Enter Value for Resource                              | LIKE           | %                                                     |                                                       |
| Enter Value for Grantable                             | LIKE           | %                                                     |                                                       |
| Show Aliases                                          | Radio buttons  | Default                                               |                                                       |
| Remote Data Source                                    | Drop-down menu |                                                       |                                                       |
| Refresh Rate (Seconds)                                | Drop-down menu | 0                                                     |                                                       |

## Cassandra Role granted to User Role

Lists all the Cassandra roles that are granted to a user.

| Domain                              |                | Based on Query                      | Main Entity                         |
|-------------------------------------|----------------|-------------------------------------|-------------------------------------|
| Cassandra Role granted to User Role |                | Cassandra Role granted to User Role | Cassandra Role granted to User Role |
| Run-Time Parameter                  | Operator       | Default Value                       |                                     |
| Period From                         | >=             | NOW -3 HOUR                         |                                     |
| Period To                           | <=             | NOW                                 |                                     |
| Enter Value for Role                | LIKE           | %                                   |                                     |
| Enter Value for Member              | LIKE           | %                                   |                                     |
| Show Aliases                        | Radio buttons  | Default                             |                                     |
| Remote Data Source                  | Drop-down menu |                                     |                                     |
| Refresh Rate (Seconds)              | Drop-down menu | 0                                   |                                     |

## Cassandra SuperUser Role

Lists all the Cassandra users with a SuperUser role.

| Domain                   |                | Based on Query           | Main Entity              |
|--------------------------|----------------|--------------------------|--------------------------|
| Cassandra SuperUser Role |                | Cassandra SuperUser Role | Cassandra SuperUser Role |
| Run-Time Parameter       | Operator       | Default Value            |                          |
| Period From              | >=             | NOW -3 HOUR              |                          |
| Period To                | <=             | NOW                      |                          |
| Enter Value for Role     | LIKE           | %                        |                          |
| Show Aliases             | Radio buttons  | Default                  |                          |
| Remote Data Source       | Drop-down menu |                          |                          |
| Refresh Rate (Seconds)   | Drop-down menu | 0                        |                          |

## CAS Deployment

This CAS reports details the Database type, OS name, Hostname and OS type.

| Domain             | Based on Query | Main Entity   |
|--------------------|----------------|---------------|
| CAS                | CAS Deployment | Not available |
| Run-Time Parameter | Operator       | Default Value |
| DB Type            | Like           | %             |
| OS_Name            | Like           | %             |
| Hostname           | Like           | %             |
| OS_Type            | Like           | %             |

## Changes (CAS)

### CAS Change Details

For each monitored item, the changes are listed in order by owner.

| Domain             | Based on Query     | Main Entity        |
|--------------------|--------------------|--------------------|
| CAS Changes        | CAS Change Details | Host Configuration |
| Run-Time Parameter | Operator           | Default Value      |

| Run-Time Parameter | Operator | Default Value |
|--------------------|----------|---------------|
| DB_Type            | Like     | %             |
| Host_Name          | Like     | %             |
| Instance_Name      | Like     | %             |
| Monitored_Item     | Like     | %             |
| OS_Type            | Like     | %             |
| Type               | Like     | %             |

#### CAS Saved Data

This report lists the data saved for each change detected. This report is sorted by host name, and then by the most recent modification time.

| Domain                    | Based on Query | Main Entity |
|---------------------------|----------------|-------------|
| CAS Changes               | CAS Saved Data | Saved Data  |
| <b>Run-Time Parameter</b> |                |             |
| Host_Name                 | Like           | %           |
| Monitored_Item            | Like           | %           |
| Saved_Data_Id             | Like           | %           |

## Configuration (CAS)

---

#### CAS Instances

This report lists CAS instance definitions (a CAS instance applies a template set to a specific CAS host). The default sort order for this report is non-standard. The sort keys are, from major to minor: Host Name (ascending), Instance (ascending) and Last Status Change (descending).

| Domain                    | Based on Query | Main Entity            |
|---------------------------|----------------|------------------------|
| CAS Config                | CAS Instances  | Monitored Item Details |
| <b>Run-Time Parameter</b> |                |                        |
| Host_Name                 | Like           | %                      |
| OS_Type                   | Like           | %                      |
| DB_Type                   | Like           | %                      |
| Instance                  | Like           | %                      |

#### CAS Instance Config

This report lists CAS instance configuration changes. The default sort order for this report is non-standard. The sort keys are, from major to minor: Host Name (ascending), Instance (ascending) and Last Status Change (descending). You can limit the output by using any of the following runtime parameters, which select all values by default.

| Domain                    | Based on Query      | Main Entity            |
|---------------------------|---------------------|------------------------|
| CAS Config                | CAS Instance Config | Monitored Item Details |
| <b>Run-Time Parameter</b> |                     |                        |
| Host_Name                 | Like                | %                      |
| OS_Type                   | Like                | %                      |
| Template_Id               | Like                | %                      |

## Connection Profiling List

---

Connection Profiling List is a group of all allowed connections (the Connection Profiling List show all connection details).

| Domain                    | Based on Query            | Main Entity   |
|---------------------------|---------------------------|---------------|
| Internal - not available  | Connection Profiling List | Client Server |
| <b>Run-time parameter</b> |                           |               |
| Query From Date           | >=                        | NOW -1 DAY    |
| Query To Date             | <=                        | NOW           |

## Connections Quarantined

---

Guardium policies can be used to terminate or quarantine connections in real time. Use threshold alerts, based on queries. See Quarantine under the Policies topic for configuration instructions.

| Domain                    | Based on Query          | Main Entity           |
|---------------------------|-------------------------|-----------------------|
| Connection Quarantine     | Connections Quarantined | Connection Quarantine |
| Period From               | >=                      | NOW -1 DAY            |
| <b>Run-Time Parameter</b> |                         |                       |
| Server IP                 | LIKE                    | %                     |
| DB User                   | LIKE                    | %                     |
| Server Name               | LIKE                    | %                     |
| Period From               | >=                      | NOW -1 DAY            |
| Period To                 | <=                      | NOW                   |

## CPU Tracker

---

Lists the Software TAP Host and number of CPUs on machines running S-TAPs.

| Domain                   | Based on Query | Main Entity   |
|--------------------------|----------------|---------------|
| Internal - not available |                | Not available |
| Run-Time Parameter       | Operator       | Default Value |
| None                     |                |               |

## CPU Usage

By default, displays the CPU usage for the last two hours. This graphical report is intended to display recent activity only. If you alter the From and To run-time parameters to include a larger timeframe, you may receive a message indicating that there is too much data. Use a tabular report to display a larger time period.

| Domain             | Based on Query | Main Entity                  |
|--------------------|----------------|------------------------------|
| Sniffer Buffer     | CPU Usage      | Sniffer Buffer Usage Monitor |
| Run-Time Parameter | Operator       | Default Value                |
| Period From        | >=             | NOW -2 HOUR                  |
| Period To          | <=             | NOW                          |

## Databases by Type/ Number of DB per type

Server type and client sources for each database type monitored.

| Domain             | Based on Query        | Main Entity   |
|--------------------|-----------------------|---------------|
| Access             | Number of db per type | Client/Server |
| Run-Time Parameter | Operator              | Default Value |
| Period From        | >=                    | NOW -1 DAY    |
| Period To          | <=                    | NOW           |

## Databases Discovered

For the reporting period, for each Discovered Port entity where the DB Type attribute value is NOT LIKE Unknown, this report lists the Probe Timestamp, Server IP, Sever Host Name, DB Type, Port, Port Type, and count of Discovered Ports for the row.

| Domain             | Based on Query       | Main Entity       |
|--------------------|----------------------|-------------------|
| Auto-discovery     | Databases Discovered | Discovered Port   |
| Run-Time Parameter | Operator             | Default Value     |
| Period From        | >=                   | NOW -1 DAY        |
| Period To          | <=                   | NOW               |
| PortNotLike        | NOT LIKE             | No default value. |

## Datamart Extraction Log

The extraction log has data about both table and file extractions. It presents:Data Mart Name, Collector IP, Server IP, from-time, to-time, ID, run started, run ended, number of records, status, error code.

## Data Sources

Lists all datasources defined: Data -Source Type, Data-Source Name , Data-Source Description, Host, Port, Service Name, User Name, Database Name, Last Connect, Shared, and Connection Properties..

You can restrict the output of this report using the Data Source Name run time parameter, which by default is set to "%" to select all datasources.

| Domain                   | Based on Query | Main Entity   |
|--------------------------|----------------|---------------|
| Internal - not available | Data-Sources   | Not available |
| Run-Time Parameter       | Operator       | Default Value |
| Data Source Name         | LIKE           | %             |
| Period From              | >=             | NOW -1 DAY    |
| Period To                | <=             | NOW           |

## Days not exported or archived

This report lists the days whose data was not exported or archived, for a system that has a daily archive or export, and if Allow purge without exporting or archiving is not selected. For more details, see [Viewing days whose data was not archived or exported](#).

| Domain                  | Based on Query                   | Main Entity    |
|-------------------------|----------------------------------|----------------|
| Catalog                 | Days not exported or archived    | Entry          |
| Run-Time Parameter      | Operator                         | Default Value  |
| Period From             | >=                               | NOW -2 WEEK    |
| Period To               | <=                               | NOW            |
| Show Aliases            | Radio buttons (On, Off, Default) | Default        |
| Remote Data Source      |                                  | Drop-down menu |
| Refresh rate in seconds |                                  | 0              |

## DB Users Mapping List

The mapping between database users (Invokers of SQL that caused a violation) and email addresses for real time alerts.

| Domain             | Based on Query        | Main Entity          |
|--------------------|-----------------------|----------------------|
| Auto-discovery     | DB Users Mapping List | Guardium Users Login |
| Run-Time Parameter | Operator              | Default Value        |
| Period From        | >=                    | NOW -1 DAY           |
| Period To          | <=                    | NOW                  |

## Default DB Users Enabled

This report details the default users found enabled after a database scan through the group of default users and list of servers supplied to the Non-credential Scan API. When an enabled user is found within a database, that occurrence of database/user is reported only once. Subsequent scans will update the timestamp and database version of the database. If a subsequent scan does not find a previously found user the timestamp remains unaffected so as to keep a history with the last time the user was found enabled on a database. Scans are run under the Classifier Listener and submitted jobs (with the non\_credential\_scan API) may be tracked using the Guardium Job Queue report.

| Domain                   | Based on Query           | Main Entity              |
|--------------------------|--------------------------|--------------------------|
| Default DB Users Enabled | Default DB Users Enabled | Default DB Users Enabled |
| Run-Time Parameter       | Operator                 | Default Value            |
| Period From              | >=                       | NOW -1 DAY               |
| Period To                | <=                       | NOW                      |

## Definitions Export/Import Log

This report lists Guardium export/import activity by Activity Type. Each row of the report contains the Activity Type, Start Time, File Name, Status, Comment, and count of log records for the row.

| Domain              | Based on Query                | Main Entity     |
|---------------------|-------------------------------|-----------------|
| Aggregation/Archive | Export-Import Definitions Log | Agg/Archive Log |
| Run-Time Parameter  | Operator                      | Default Value   |
| Period From         | >=                            | NOW -1 DAY      |
| Period To           | <=                            | NOW             |

## Discovered Instances

This S-TAP report details the following information:

Timestamp, Host, Protocol, Port Min, Port Max, KTAP DB Port, Instance Names, Client, Exclude Client, Proc Names, Named Pipe, DB Install Dir, Proc Name, DB2® Shared Mem Adjustment, DB2 Shared Mem Client Position, DB2 Shared Mem Size, Unix Socket, DB User, DB Version.

Columns are populated as relevant, according to the database type.

| Domain               | Based on Query       | Main Entity          |
|----------------------|----------------------|----------------------|
| Discovered Instances | Discovered Instances | Discovered Instances |
| Run-Time Parameter   | Operator             | Default Value        |
| Period From          | >=                   | NOW -1 DAY           |
| Period To            | <=                   | NOW                  |

## Discovered Instances Rules Add or Replace Log

This report details the following information: Timestamp, Host, Result, Report Only.

| Domain                               | Based on Query                                | Main Entity                        |
|--------------------------------------|-----------------------------------------------|------------------------------------|
| Discovered Instances                 | Discovered Instances Rules Add or Replace Log | Discovered Instances Rules Results |
| Run-Time Parameter                   | Operator                                      | Default Value                      |
| Period From                          | >=                                            | NOW -3 HOUR                        |
| Period To                            | <=                                            | NOW                                |
| Enter Value for Report Only (Yes/No) | Like                                          | %                                  |
| Show Aliases                         | Radio buttons (On, Off, Default)              | Default                            |
| Remote Data Source                   |                                               | Drop-down menu                     |
| Refresh rate in seconds              |                                               | 0                                  |

## Discovered Instances Rules Results

This report details the following information:

Timestamp, Host, Result Message, Result Type, Report Only, Identifier, Discovered, Protocol, Port Min, Port Max, Instance Name, Named Pipe, DB Install Dir, Proc Name, DB2 Shared Mem Adjustment , DB2 Shared Mem Client Position, DB2 Shared Mem Size, Unix Socket, DB User, DB Version.

| Domain               | Based on Query                     | Main Entity                        |
|----------------------|------------------------------------|------------------------------------|
| Discovered Instances | Discovered Instances Rules Results | Discovered Instances Rules Results |
| Run-Time Parameter   | Operator                           | Default Value                      |
| Period From          | >=                                 | NOW -3 HOUR                        |
| Period To            | <=                                 | NOW                                |

| Run-Time Parameter                   | Operator                         | Default Value  |
|--------------------------------------|----------------------------------|----------------|
| Period From                          | >=                               | NOW -3 HOUR    |
| Period To                            | <=                               | NOW            |
| Enter Value for Report Only (Yes/No) | Like                             | %              |
| Show Aliases                         | Radio buttons (On, Off, Default) | Default        |
| Remote Data Source                   |                                  | Drop-down menu |
| Refresh rate in seconds              |                                  | 0              |

## Dropped Requests

Tracks requests dropped by an inspection engine (Exception Description = Dropped database request). Under extremely rare, high-volume situations some requests may be lost. When this happens, the sessions from which the requests were lost are listed in the Dropped Requests report.

| Domain             | Based on Query   | Main Entity   |
|--------------------|------------------|---------------|
| Exceptions         | Dropped Requests | Exception     |
| Run-Time Parameter | Operator         | Default Value |
| Period From        | >=               | NOW -1 DAY    |
| Period To          | <=               | NOW           |

## Enterprise S-TAP Association History

Enterprise S-TAP Association History reports on how long the S-TAP reported to the specific Guardium system in the Load balancer environment.

In order to see this report, you must schedule the CustomTableStapAssocicationJob. (It is not automatically scheduled by default.) For example, to schedule this job to run hourly, run the command: **grdapi schedule\_job cronString="0 0/1 \* 1,2,3,4,5,6,7" jobType="customTableStapAssocication"**

If you set the job to run hourly, you'll see S-TAP association changes with a one hour delay. If you need to see the changes sooner, you can schedule this job to run at more frequent intervals. However, there can be a tradeoff in central manager environments with a large number of S-TAPs, between frequency of reports and load on the system. If the S-TAPs move frequently, running this job every five minutes might burden the central manager. Set the frequency according to your needs, and your environment. To set the job to run every five minutes, run the command: **grdapi schedule\_job cronString="0 0/5 0/1 \* 1,2,3,4,5,6,7" jobType="customTableStapAssocication"**

## Enterprise Buffer Usage Monitor

This report shows the aggregate of sniffer buffer usage from all managed units. There is a need to set the schedule for the upload. See the description of the Sniffer Buffer Usage entity for a description of the fields listed on this report.

| Domain                  | Based on Query          | Main Entity          |
|-------------------------|-------------------------|----------------------|
| Enterprise Buffer Usage | Enterprise Buffer Usage | Sniffer Buffer Usage |
| Run-Time Parameter      | Operator                | Default Value        |
| Period From             | >=                      | NOW -1 DAY           |
| Period To               | <=                      | NOW                  |

## Enterprise S-TAP (Detailed) View

See [S-TAP Info \(Central Manager\)](#) for information on this report.

## Enterprise S-TAP View

See [S-TAP Info \(Central Manager\)](#) for information on this report.

## Exception Count

For the reporting period, the total number of exceptions logged.

| Domain             | Based on Query  | Main Entity   |
|--------------------|-----------------|---------------|
| Exceptions         | Exception Count | Exception     |
| Run-Time Parameter | Operator        | Default Value |
| Period From        | >=              | NOW -1 DAY    |
| Period To          | <=              | NOW           |

## Export Sensitive Data to Discovery

Guardium and InfoSphere® Discovery have mechanisms for the Classification of Sensitive Data.

A bidirectional interface is provided to transfer the identified sensitive data from Guardium to InfoSphere Discovery and from InfoSphere Discovery to Guardium.

This data will be transferred via CSV files. See [External data correlation](#) for further information.

| Domain                   | Based on Query                     | Main Entity                    |
|--------------------------|------------------------------------|--------------------------------|
| Internal - not available | Export Sensitive Data to Discovery | Classification Process Results |
| Run-Time Parameter       | Operator                           | Default Value                  |
| Period From              | >=                                 | NOW -3 HOURS                   |

| Run-Time Parameter | Operator | Default Value |
|--------------------|----------|---------------|
| Period To          | <=       | NOW           |
| Rule Description   | LIKE     |               |
| Schema             | LIKE     |               |

## External Tickets

---

Displays details of tickets that are created in Guardium and sent to external sources such as ServiceNow or Resilient.

| Domain                          | Based on Query  | Main Entity     |
|---------------------------------|-----------------|-----------------|
| Internal - not available        | External Ticket | External Ticket |
| Run-Time Parameter              | Operator        | Default Value   |
| Period From                     | >=              | NOW -3 HOUR     |
| Period To                       | <=              | NOW             |
| Enter Value for Guardium Source | LIKE            | %               |
| Enter Value for Ticket Number   | LIKE            | %               |
| Refresh rate in seconds         |                 | 0               |

## FAM Config Change

---

Displays details about the changes in the File Activity Monitor (FAM) configuration.

| Domain                  | Based on Query                   | Main Entity    |
|-------------------------|----------------------------------|----------------|
| Exceptions              | FAM Config Change                | Exception      |
| Run-Time Parameter      | Operator                         | Default Value  |
| Period From             | >=                               | NOW -3 HOUR    |
| Period To               | <=                               | NOW            |
| Show Aliases            | Radio buttons (On, Off, Default) | Default        |
| Remote Data Source      |                                  | Drop-down menu |
| Refresh rate in seconds |                                  | 0              |

## FAM Progress

---

Displays details about the progress of File Discovery, Entitlement and Classification (FDEC) scans for NAS and Sharepoint.

Note: FDEC does not provide live updates for removed objects. The numbers in the Removed Objects column always reflects the total number of removed objects.

| Domain                                | Based on Query | Main Entity   |
|---------------------------------------|----------------|---------------|
| Internal - not available              | Not available  | Not available |
| Run-Time Parameter                    | Operator       | Default Value |
| Period From                           | >=             | NOW -3 HOUR   |
| Period To                             | <=             | NOW           |
| Enter Value for NAS or SP Host Name   | Like           | %             |
| Enter Value for Source Directory Path | Like           | %             |
| Refresh rate in seconds               |                | 0             |

## Full SQL

---

This report summarizes SQL commands performed by the user, or that run on the database (depending on the source).

| Domain                       | Based on Query                   | Main Entity    |
|------------------------------|----------------------------------|----------------|
| Access                       | Full SQL                         | Full SQL       |
| Run-Time Parameter           | Operator                         | Default Value  |
| Period From                  | >=                               | NOW -3 HOUR    |
| Period To                    | <=                               | NOW            |
| Enter Value for Service Name | Like                             | %              |
| Enter Value for OS User      | Like                             | %              |
| Enter Value for DB User Name | Like                             | %              |
| Enter Value for Server IP    | Like                             | %              |
| Show Aliases                 | Radio buttons (On, Off, Default) | Default        |
| Remote Data Source           |                                  | Drop-down menu |
| Refresh rate in seconds      |                                  | 0              |

## Full SQL - Data Tampering

---

This is a filtered view of the full SQL report, showing only the results for data tampering.

| Run-Time Parameter           | Operator | Default Value |
|------------------------------|----------|---------------|
| Period From                  | >=       | NOW -3 HOUR   |
| Period To                    | <=       | NOW           |
| Enter Value for Service Name | Like     | %             |

| Run-Time Parameter           | Operator                         | Default Value  |
|------------------------------|----------------------------------|----------------|
| Enter Value for DB User Name | Like                             | %              |
| Enter Value for OS User      | Like                             | %              |
| Enter Value for Service Name | Like                             | %              |
| Show Aliases                 | Radio buttons (On, Off, Default) | Default        |
| Remote Data Source           |                                  | Drop-down menu |
| Refresh rate in seconds      |                                  | 0              |

## Full SQL - Massive Grants

This is a filtered view of the full SQL report, showing only the results for massive grants.

| Run-Time Parameter           | Operator                         | Default Value  |
|------------------------------|----------------------------------|----------------|
| Period From                  | >=                               | NOW -3 HOUR    |
| Period To                    | <=                               | NOW            |
| Enter Value for Server IP    | Like                             | %              |
| Enter Value for DB User Name | Like                             | %              |
| Enter Value for OS User      | Like                             | %              |
| Enter Value for Service Name | Like                             | %              |
| Show Aliases                 | Radio buttons (On, Off, Default) | Default        |
| Remote Data Source           |                                  | Drop-down menu |
| Refresh rate in seconds      |                                  | 0              |

## Full SQL - Possible data leak

This is a filtered view of the full SQL report, showing only the results for possible data leaks.

| Run-Time Parameter           | Operator                         | Default Value  |
|------------------------------|----------------------------------|----------------|
| Period From                  | >=                               | NOW -3 HOUR    |
| Period To                    | <=                               | NOW            |
| Enter Value for Server IP    | Like                             | %              |
| Enter Value for DB User Name | Like                             | %              |
| Enter Value for OS User      | Like                             | %              |
| Enter Value for Service Name | Like                             | %              |
| Show Aliases                 | Radio buttons (On, Off, Default) | Default        |
| Remote Data Source           |                                  | Drop-down menu |
| Refresh rate in seconds      |                                  | 0              |

## Full SQL - Schema tampering

This is a filtered view of the full SQL report, showing only the results for schema tampering.

| Run-Time Parameter           | Operator                         | Default Value  |
|------------------------------|----------------------------------|----------------|
| Period From                  | >=                               | NOW -3 HOUR    |
| Period To                    | <=                               | NOW            |
| Enter Value for Server IP    | Like                             | %              |
| Enter Value for DB User Name | Like                             | %              |
| Enter Value for OS User      | Like                             | %              |
| Enter Value for Service Name | Like                             | %              |
| Show Aliases                 | Radio buttons (On, Off, Default) | Default        |
| Remote Data Source           |                                  | Drop-down menu |
| Refresh rate in seconds      |                                  | 0              |

## Full SQL By Client IP

| Domain                  | Based on Query                   | Main Entity    |
|-------------------------|----------------------------------|----------------|
| Access                  | Full SQL By Client IP            | Full SQL       |
| Run-Time Parameter      | Operator                         | Default Value  |
| Period From             | >=                               | NOW -3 HOUR    |
| Period To               | <=                               | NOW            |
| Show Aliases            | Radio buttons (On, Off, Default) | Default        |
| Remote Data Source      |                                  | Drop-down menu |
| Refresh rate in seconds |                                  | 0              |

## Full SQL by DB User

| Domain             | Based on Query      | Main Entity   |
|--------------------|---------------------|---------------|
| Access             | Full SQL by DB user | Full SQL      |
| Run-Time Parameter | Operator            | Default Value |

| Run-Time Parameter           | Operator                         | Default Value  |
|------------------------------|----------------------------------|----------------|
| Period From                  | >=                               | NOW -3 HOUR    |
| Period To                    | <=                               | NOW            |
| Enter Value for DB User Name | Like                             | %              |
| Show Aliases                 | Radio buttons (On, Off, Default) | Default        |
| Remote Data Source           |                                  | Drop-down menu |
| Refresh rate in seconds      |                                  | 0              |

## Guardium Job Queue

Displays the Guardium Job Queue. Previously known as Classifier/Assessment Job Queue. For each job, it lists the Process Run ID, Process Type, Status, Guardium Job Process Id, Report Result Id, Guardium Job Description, Audit Task Description, Queue Time, Start Time, End Time, and Data Sources.

| Domain                          | Based on Query                         | Main Entity    |
|---------------------------------|----------------------------------------|----------------|
| Internal - not available        | Guardium Job Queue                     | Not available  |
| <b>Run-Time Parameter</b>       |                                        |                |
| Period From                     | >=                                     | NOW -1 DAY     |
| Period To                       | <=                                     | NOW            |
| Enter Value for Job Description | Like                                   | %              |
| Enter Value for Process Type    | Like                                   | %              |
| Show Aliases                    | Radio buttons (On, Off, Both, Default) | Default        |
| Remote Data Source              |                                        | Drop-down menu |
| Refresh Rate (seconds)          |                                        | 0              |

The job queue

Assessments and Classifications run in their own separate process called the job queue. Jobs are queued and have their status maintained while a listener periodically polls the queue looking for waiting jobs to run.

Stopping

Running jobs, when right-clicked for drill-down, there is an option to stop the running job and cancel it. The job can not be restarted at this point.

Halting

Running jobs are monitored to reduce the number of hung jobs that might cause the job queue to become overloaded. If a job is inactive for 30 minutes, the listener is terminated and restarted, effectively stopping the operation of a job. Before the listener is restarted, a process called the cleaner runs, the status is set from RUNNING to HALTED, and then the listener is restarted. A status of HALTED means the job was not able to run to completion.

Resubmitting

Sometimes the listener gets restarted for reasons other than a job hanging, for example rebooting the machine. When the cleaner halts the running jobs, it will see if the job has responded in the past 8 minutes. If it has, the job will be copied and that copy will be resubmitted onto the job queue. The original halted will still display on the queue, and still have the results it was able to process available.

Monitoring

The mechanism by which jobs maintain their active status is by touching the timestamp on the job queue record. It is important to note that the job queue record is used for the entire job. Each individual classifier rule or assessment test interacts with the timestamp for its parent process, and they do not have individual timestamps that are monitored.

The classifier will update its timestamp before every rule is tested and after every SQL operation. For example, if the classifier is scanning the data in a database that supports paging, it will touch the timestamp after each batch of data is brought back from the database. This is because, depending on the state of the target database, the classifier has the potential to invoke some long-running queries that will be limited to 30 minutes of execution.

Assessments touch the timestamp after each test in the assessment is evaluated. Most assessment tests run in a few seconds or less.

Observed Tests

The exception to the relatively quick-running assessment tests is the category of observed assessment tests. These tests are based on queries and reports that use the internal sniffing data on the Guardium appliance and can run for longer periods of time and are unable to update the timestamp while they are in process. Therefore, observed assessment tests have their timestamps set two hours into the future when they are started, essentially giving them two hours and thirty minutes to run to conclusion. This can be confusing when looking at the job queue and seeing the timestamp set to a time in the future. Just like any other assessment test, when the observed test ends, the timestamp will be touched. If the next test is an observed test, the timestamp will once again be set two hours into the future. Otherwise, the timestamp will be set to the current time.

## Guardium usage summary

Displays a list S-TAP hosts, number of processors per the Guardium License Metric Tool (ILMT), and the estimated number of processor value units (PVUs).

To calculate the accurate number of PVUs, see <https://www-112.ibm.com/software/howtobuy/passportadvantage/pvucalculator/pvucalc.wss>

| Domain                    | Based on Query                         | Main Entity    |
|---------------------------|----------------------------------------|----------------|
| Internal-not available    | Guardium usage summary                 | Not available  |
| <b>Run-Time Parameter</b> |                                        |                |
| Period From               | >=                                     | NOW -3 HOUR    |
| Period To                 | <=                                     | NOW            |
| Remote Data Source        |                                        | Drop-down menu |
| Show Aliases              | Radio buttons (On, Off, Both, Default) | Default        |

| Run-Time Parameter     | Operator | Default Value |
|------------------------|----------|---------------|
| Refresh Rate (seconds) |          | 0             |

## GIM Clients Status

Displays a list of GIM clients, including the client name, OS, vendor, installation date, module name, module version, module state, module schedule, and the system the GIM module reports to.

| Domain             | Based on Query     | Main Entity   |
|--------------------|--------------------|---------------|
| GIM Clients Status | GIM Clients Status | GIM Clients   |
| Run-Time Parameter | Operator           | Default Value |
| Client Name        | %                  | Not available |
| Client OS          | %                  | Not available |

## GIM Events List

Displays a list of GIM Events.

| Domain             | Based on Query | Main Entity   |
|--------------------|----------------|---------------|
| GIM Events         | GIM Events     | GIM Events    |
| Run-Time Parameter | Operator       | Default Value |
| Period From        | >=             | NOW -1 DAY    |
| Period To          | <=             | NOW           |

## GIM Installed Modules

Displays a list of installed GIM Modules.

Note: This report shows the modules that have been associated with the host. If a module has been assigned to a host, the assigned version does appear in this report, even if the module has not yet been scheduled or installed. To check the currently installed module, review the GIM Client Status report.

| Domain             | Based on Query     | Main Entity    |
|--------------------|--------------------|----------------|
| GIM Installed Base | GIM Installed Base | GIM Installed  |
| Run-Time Parameter | Operator           | Default Value  |
| none               | not applicable     | not applicable |

## Group Usage Report

Displays the list of all defined groups and all the entities that rely on each group.

## Guardium API Exceptions

Displays a time stamp and description of all GuardAPI exceptions. These are jobs where the Exception Type ID is GUARD\_API\_EXCEPTION.

| Domain             | Based on Query          | Main Entity   |
|--------------------|-------------------------|---------------|
| Exception          | Guardium API Exceptions | Exception     |
| Run-Time Parameter | Operator                | Default Value |
| Period From        | >=                      | NOW -1 DAY    |
| Period To          | <=                      | NOW           |

## Guardium entitlement consolidation report (using ILMT)

This report provides details on active/inactive S-TAP installed on the data server. If the ILMT agent is installed, the report shows the processors value of the data server. If the ILMT agent is not installed, the processor value is blank. This report helps indicate the processor value of the server with an installed, and active S-TAP. The ILMT agent provides the processor value once an ILMT agent is installed; this report does not replace ILMT requirements in any sense (Follow ILMT compliance and audit requirements).

| Domain                 | Based on Query                            | Main Entity    |
|------------------------|-------------------------------------------|----------------|
| Internal-not available | Guardium entitlement consolidation report | Not available  |
| Run-Time Parameter     | Operator                                  | Default Value  |
| Period From            | >=                                        | NOW -3 HOUR    |
| Period To              | <=                                        | NOW            |
| Remote Data Source     |                                           | Drop-down menu |
| Show Aliases           | Radio buttons (On, Off, Both, Default)    | Default        |
| Refresh Rate (seconds) |                                           | 0              |

## Guardium Group Details

For the reporting period, each row of the report lists a group member. The columns contain the following information: Group Description, Group Type, Group Subtype, Timestamp (from the Group Member entity), Group Member, and count of Group Member entities for the row. The value of the timestamp is set to the current time whenever the record is updated.

You can restrict the output of this report using the run-time parameters, both of which are used with the LIKE operator and a default value of %, which selects all values.

| Domain             | Based on Query         | Main Entity    |
|--------------------|------------------------|----------------|
| Group              | Guardium Group Details | Group Member   |
| Run-Time Parameter | Operator               | Default Value  |
| Group Description  | LIKE                   | %              |
| Group Type         | LIKE                   | %              |
| Period From        | >=                     | NOW -100 MONTH |
| Period To          | <=                     | NOW            |

## Guardium Users

Lists each user, date of last activity, and number of roles assigned. For each user, you can drill down to the Record Details report to see the roles assigned to that user.

| Domain                   | Based on Query | Main Entity    |
|--------------------------|----------------|----------------|
| Internal - not available | User Role      | Not available  |
| Run-Time Parameter       | Operator       | Default Value  |
| Period From              | >=             | NOW -100 MONTH |
| Period To                | <=             | NOW            |

## Host History (CAS)

This report lists CAS host events. The default sort order for this report is non-standard. The sort keys are, from major to minor: Host Name (ascending), Instance and Event Time (descending).

| Domain             | Based on Query   | Main Entity   |
|--------------------|------------------|---------------|
| CAS Host History   | CAS Host History | Host Event    |
| Run-Time Parameter | Operator         | Default Value |
| Host_Name          | Like             | %             |
| OS_Type            | Like             | %             |
| Event_Type         | Like             | %             |

## Inactive Inspection Engines

Lists all inactive inspection engines

| Domain                   | Based on Query              | Main Entity               |
|--------------------------|-----------------------------|---------------------------|
| Internal - not available | Inactive Inspection Engines | S-TAP Verification Header |
| Run-Time Parameter       | Operator                    | Default Value             |
| Query from date          | >=                          | NOW -3 HOUR               |
| Query to date            | >=                          | NOW                       |

## Inactive S-TAPs Since

Lists all inactive S-TAPs defined on the system. It has a single run-time parameter: Period From, which is set to now -1 hour by default. Use this parameter to control how you want to define inactive. This report contains the same columns of data for the S-TAP Status report with the addition of a count for each row of the report.

| Domain                   | Based on Query        | Main Entity   |
|--------------------------|-----------------------|---------------|
| Internal - not available | Inactive S-TAPs Since | Not available |
| Run-Time Parameter       | Operator              | Default Value |
| Period From              | >=                    | NOW -1 HOUR   |

## Installed Patches

Displays the patches: Patch Number, Guardium Version, Patch Description, Patch Dependencies, Creation Date, Request Received, Installed By, Status, Status Description, Timestamp, Requested Schedule.

| Domain                  | Based on Query    | Main Entity     |
|-------------------------|-------------------|-----------------|
| Installed Patches       | Installed Patches | Installed Patch |
| Run-Time Parameter      | Operator          | Default Value   |
| Refresh rate in seconds |                   | 0               |

## Investigation dashboard issues

This report displays all Investigation dashboard issues that Monitoring and automatic recovery discovered, including those that are open, in progress, and fixed.

You can limit the output by setting the Guardium Host Name run-time parameter, which is set to % by default (to select all servers). This reduces the number of issues you see in the report.

| Domain                         | Based on Query                 | Main Entity                    |
|--------------------------------|--------------------------------|--------------------------------|
| Investigation dashboard issues | Investigation dashboard issues | Investigation dashboard issues |
| Run-Time Parameters            | Operator                       | Default Value                  |
| Period From                    | >=                             | NOW -3 HOUR                    |

|           |      |     |
|-----------|------|-----|
| Period To | <=   | NOW |
| Host Name | LIKE | %   |

## Investigation dashboard issues in recovery

This report displays the Investigation dashboard issues that Monitoring and automatic recovery is currently trying to fix.

Condition – Investigation Dashboard issue

Status = 'Recovery in progress'

You can limit the output by setting the Guardium Host Name run-time parameter, which is set to % by default (to select all servers). This reduces the number of issues you see in the report.

| Domain                         | Based on Query                             | Main Entity                    |
|--------------------------------|--------------------------------------------|--------------------------------|
| Investigation dashboard issues | Investigation dashboard issues in recovery | Investigation dashboard issues |
| Run-Time Parameters            | Operator                                   | Default Value                  |
| Period From                    | >=                                         | NOW -3 HOUR                    |
| Period To                      | <=                                         | NOW                            |
| Host Name                      | LIKE                                       | %                              |

## Investigation dashboard open issues

This report displays the Investigation dashboard issues that Monitoring and automatic recovery was not able to fix that require manual intervention to resolve

Condition – Investigation Dashboard

issue status = 'Error'

You can limit the output by setting the Guardium Host Name run-time parameter, which is set to % by default (to select all servers). This reduces the number of issues you see in the report.

| Domain                         | Based on Query                      | Main Entity                    |
|--------------------------------|-------------------------------------|--------------------------------|
| Investigation dashboard issues | Investigation dashboard open issues | Investigation dashboard issues |
| Run-Time Parameters            | Operator                            | Default Value                  |
| Period From                    | >=                                  | NOW -3 HOUR                    |
| Period To                      | <=                                  | NOW                            |
| Host Name                      | LIKE                                | %                              |

## Logged R/T Alerts

For the reporting period, the total number of logged real time alerts, listed by rule description.

| Domain             | Based on Query    | Main Entity           |
|--------------------|-------------------|-----------------------|
| Policy Violations  | Logged R/T Alerts | Policy Rule Violation |
| Run-Time Parameter | Operator          | Default Value         |
| Period From        | >=                | NOW -1 DAY            |
| Period To          | <=                | NOW                   |

## Logged Threshold Alerts

For the reporting period, the total number of threshold alerts logged.

| Domain             | Based on Query | Main Entity             |
|--------------------|----------------|-------------------------|
| Alert              | Logged Alerts  | Threshold Alert Details |
| Run-Time Parameter | Operator       | Default Value           |
| Period From        | >=             | NOW -1 DAY              |
| Period To          | <=             | NOW                     |

## Logging Collectors (valid only from aggregation unit)

The Logging Collectors report appears under the Daily Monitor Tab and it is valid only on an aggregator unit. This report shows the number of sessions per Server IP, per collector and per day. For example: on May 19, aggregator #1 collected 100 sessions for Server 192.168.x.x1, 50 sessions for Server 192.168.x.x2; aggregator #2 collected 30 sessions for Server 192.168.x.x3, 90 sessions for Server 192.168.x.x4; etc.

| Domain             | Based on Query     | Main Entity        |
|--------------------|--------------------|--------------------|
| Exceptions         | Logging Collectors | Logging Collectors |
| Run-Time Parameter | Operator           | Default Value      |
| Period From        | >=                 | NOW -1 DAY         |
| Period To          | <=                 | NOW                |

## Logins to Guardium

All values for this report are from the Guardium Logins entity. For the reporting period, each row of the report lists the User Name, Login Succeeded (1= Successful, 0=Failed, -1 =password expired, -2 = login from different IP), Login Date And Time, Logout Date And Time (which is blank if the user has not yet logged out), Host Name,

Remote Address (of the user) and count of logins for the row.

| Domain             | Based on Query  | Main Entity          |
|--------------------|-----------------|----------------------|
| Guardium Logins    | Guardium Logins | Guardium Users Login |
| Run-Time Parameter | Operator        | Default Value        |
| Host Name          | LIKE            | %                    |
| Period From        | >=              | NOW -1 DAY           |
| Period To          | <=              | NOW                  |

## Managed Units (Central Manager)

Enterprise report on a Central Manager that shows which managed units are up. Use this report in a Statistical Alert to send an email to an ADMIN anytime a managed unit is down.

| Domain                   | Based on Query | Main Entity                      |
|--------------------------|----------------|----------------------------------|
| Internal - not available | Managed Units  | Managed Units                    |
| Run-Time Parameter       | Operator       | Default Value                    |
| Host Name                | LIKE           | %                                |
| Remote Data Source       |                | Drop-down menu                   |
| Show Aliases             |                | Radio buttons (On, Off, Default) |

## NAS File Activities

Displays details about the file activity in Network-Attached Storage (NAS) devices.

| Domain                 | Based on Query                   | Main Entity    |
|------------------------|----------------------------------|----------------|
| Access                 | NAS File Activities              | Object/Command |
| Run-Time Parameter     | Operator                         | Default Value  |
| Period From            | >=                               | NOW -3 HOUR    |
| Show Aliases           | Radio buttons (On, Off, Default) | Default        |
| Remote Data Source     |                                  | Drop-down menu |
| Refresh Rate (seconds) |                                  | 0              |

## Number of Active Audit Processes

Number of active Guardium audit processes. When central management is used, this report contains data only on the Central Manager, and is empty on all managed units (the standard message, No data found for requested query, displays). There are no run-time parameters for this report.

| Domain        | Based on Query             | Main Entity   |
|---------------|----------------------------|---------------|
| Audit Process | Number of Active Processes | Audit Process |

## Oracle Unified Audit Activity

This report presents the server, client, and database details for the logged Oracle traffic.

| Domain                 | Based on Query                | Main Entity            |
|------------------------|-------------------------------|------------------------|
| Access                 | Oracle Unified Audit Activity | STAP SQL Configuration |
| Run-Time Parameter     | Operator                      | Default Value          |
| Period From            | >=                            | NOW -3 HOUR            |
| Period To              | <=                            | NOW                    |
| Refresh Rate (seconds) |                               | 0                      |

## Oracle Unified Audit (S-TAP configuration) Activity

This report shows details of the S-TAP and host configurations for Oracle Unified Auditing, the data pull interval and number of rows, and the timeout.

| Domain                 | Based on Query                                      | Main Entity              |
|------------------------|-----------------------------------------------------|--------------------------|
| S-TAP Status           | Oracle Unified Audit (S-TAP Configuration) Activity | Client/Server by Session |
| Run-Time Parameter     | Operator                                            | Default Value            |
| Period From            | >=                                                  | NOW -3 HOUR              |
| Period To              | <=                                                  | NOW                      |
| Refresh Rate (seconds) |                                                     | 0                        |

## Outstanding Audit Process Reviews

Number of outstanding Guardium audit processes, listed by Guardium users.

Table 1. Outstanding Audit Process Reviews

| Domain        | Based on Query                    | Main Entity             |
|---------------|-----------------------------------|-------------------------|
| Audit Process | Outstanding Audit Process Reviews | Task Results To-Do List |

## Primary Guardium Host Change Log

Log of primary host changes for S-TAPs. The primary host is the Guardium unit to which the S-TAP sends data. Each line of the report lists the S-TAP Host, Guardium Host Name, Period Start and Period End.

| Domain                   | Based on Query                 | Main Entity   |
|--------------------------|--------------------------------|---------------|
| Internal - not available | Primary SGuard host change log | Not available |
| Run-Time Parameter       | Operator                       | Default Value |
| Period From              | >=                             | NOW -1 DAY    |
| Period To                | <=                             | NOW           |

## Query Entities and Attributes

This report lists all the entities and attributes in Guardium reports and was created to simplify the linkage between the Guardium attributes to the GuardAPI calls.

Use this report to also invoke create\_constant\_attribute, create\_api\_parameter\_mapping, delete\_api\_parameter\_mapping, or list\_param\_mapping\_for\_function.

| Domain                                                                                                                                                                                                                                    | Based on Query                               | Main Entity                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------------------|
| Any of Guardium reporting domains                                                                                                                                                                                                         | Any of the entities for the reporting domain | Any of the attributes within the entity |
| Run-Time Parameter                                                                                                                                                                                                                        | Operator                                     | Default Value                           |
| Report Name Like<br>if <> '%' it will show only the domain/entity and attributes used by reports that match the new parameter.<br>IF '%' then all domains, queries and attributes are displayed (including those not used by any report). | not applicable                               | not applicable                          |

## Replay Statistics

This report shows Replay Statistics for Execution Start/End Date; Configuration Name; Schedule Setup Name; Job Status; Statistic Description; Session ID; Successful Queries; Failed Queries; Total Queries; Type; Active/Waiting/Completed Tasks.

| Domain                  | Based on Query    | Main Entity              |
|-------------------------|-------------------|--------------------------|
| Replay Results Tracking | Replay Statistics | Replay Result Statistics |
| Run-Time Parameter      | Operator          | Default Value            |
| Query from date         | >=                | NOW -1 DAY               |
| Query to date           | <=                | NOW                      |
| Session                 | >=                | Not available            |
| Session                 | <=                | Not available            |

## Replay Summary

For the reporting period, a measure of what query failed or succeeded. Checkmark required in Replay Configuration for Query Failed or Query Succeeded.

| Domain              | Based on Query | Main Entity    |
|---------------------|----------------|----------------|
| Replay Results      | Replay Summary | Replay Results |
| Run-Time Parameter  | Operator       | Default Value  |
| Query from date     | >=             | NOW -1 DAY     |
| Query to date       | <=             | NOW            |
| Results status      | %              | Not available  |
| Schedule setup name | %              | Not available  |

## Request Rate

By default, displays the request rate for the last two hours. This graphical report is intended to display recent activity only. If you alter the run-time parameters to include a larger timeframe, you may receive a message indicating that there is too much data. Use a tabular report to display a larger time period.

| Domain             | Based on Query | Main Entity                  |
|--------------------|----------------|------------------------------|
| Sniffer Buffer     | Request Rate   | Sniffer Buffer Usage Monitor |
| Run-Time Parameter | Operator       | Default Value                |
| Period From        | >=             | NOW -2 HOUR                  |
| Period To          | <=             | NOW                          |

## Restored Data

This report has two columns: RESTORED\_DAY and EXPIRATION\_DATE. When the user restores data from archive, this table is populated according to the data restored and the duration specified for keeping this data. The purge process looks at this table to determine what data can be purged and cleans up records that expired. RESTORED\_DAY is the date of the data that was restored and is in the past. EXPIRATION\_DATE is the date when this data will be purged and is a date in the future.

| Domain             | Based on Query | Main Entity   |
|--------------------|----------------|---------------|
| Restored Data      | Restored Data  | Restored Data |
| Run-Time Parameter | Operator       | Default Value |
| Period From        | >=             | NOW -10 DAY   |

| Run-Time Parameter | Operator | Default Value |
|--------------------|----------|---------------|
| Period To          | <=       | NOW +10 DAY   |

## Risky Users - Connection Profiling List

This report is the Connection Profiling List, filtered for risky users.

| Domain                                       | Based on Query            | Main Entity                |
|----------------------------------------------|---------------------------|----------------------------|
| Access                                       | Connection Profiling List | Client Server              |
| Run-Time Parameter                           | Operator                  | Default Value              |
| Query from date                              | >=                        | NOW -1 DAY                 |
| Query to date                                | <=                        | NOW                        |
| Client IP/Src App/DB User/Server IP/Svc Name | not like group            | Connection Profiling List  |
| Client IP/Src App/DB User/Server IP/Svc Name | like group                | Risk Spotter - Risky Users |

## Risky Users - Policy Violation

This report is the Policy Violation, filtered for risky users.

| Domain                                       | Based on Query                 | Main Entity                |
|----------------------------------------------|--------------------------------|----------------------------|
| Policy Violations                            | Risky Users - Policy Violation | Policy Rule Violation      |
| Run-Time Parameter                           | Operator                       | Default Value              |
| Client IP/Src App/DB User/Server IP/Svc Name | like group                     | Risk Spotter - Risky Users |
| Policy Rule Violation:Severity               | >=                             | 1                          |

## Risky Users - SQL Errors

This report is the SQL Errors report, filtered for risky users.

| Domain                                       | Based on Query           | Main Entity                |
|----------------------------------------------|--------------------------|----------------------------|
| Exception                                    | Risky Users - SQL Errors | Exception                  |
| Run-Time Parameter                           | Operator                 | Default Value              |
| Exception Type:Exception Type Description    | like                     | Database%Server%           |
| Client IP/Src App/DB User/Server IP/Svc Name | like group               | Risk Spotter - Risky Users |

## Runtime Sensitive Object Identifier

Displays output from the Runtime Sensitive Object Identifier session level policy. For more information, see [Runtime sensitive-object identification](#).

| Domain                              | Based on Query                      | Main Entity                         |
|-------------------------------------|-------------------------------------|-------------------------------------|
| Runtime Sensitive Object Identifier | Runtime Sensitive Object Identifier | Runtime Sensitive Object Identifier |

## Scheduled Job Exceptions

Displays a timestamp and the description for each scheduled job exception (including assessment errors).. These are jobs where the Exception Type ID is one of the following: SCHED\_JOB\_EXCEPTION, ASSESSMENT\_EXCEPTION, or ASMT\_ERROR.

| Domain             | Based on Query | Main Entity          |
|--------------------|----------------|----------------------|
| Sniffer Buffer     | CPU Usage      | Sniffer Buffer Usage |
| Run-Time Parameter | Operator       | Default Value        |
| Period From        | >=             | NOW -2 HOUR          |
| Period To          | <=             | NOW                  |

## Scheduled Jobs

Displays the list of currently scheduled jobs.

| Domain                   | Based on Query | Main Entity   |
|--------------------------|----------------|---------------|
| Internal - not available | Scheduled Jobs | Not available |

## Session Count

For the reporting period, the total number of different sessions open.

| Domain             | Based on Query | Main Entity   |
|--------------------|----------------|---------------|
| Access             | Session Count  | Session       |
| Run-Time Parameter | Operator       | Default Value |
| Period From        | >=             | NOW -1 DAY    |
| Period To          | <=             | NOW           |

## SharePoint File Activities

Displays details about the file activity in a SharePoint environment.

| Domain                 | Based on Query                   | Main Entity    |
|------------------------|----------------------------------|----------------|
| Access                 | SharePoint File Activities       | Object/Command |
| Run-Time Parameter     | Operator                         | Default Value  |
| Period From            | >=                               | NOW -3 HOUR    |
| Show Aliases           | Radio buttons (On, Off, Default) | Default        |
| Remote Data Source     |                                  | Drop-down menu |
| Refresh Rate (seconds) |                                  | 0              |

## SQL Count

For the reporting period, the total number of different SQL commands issued.

| Domain             | Based on Query | Main Entity   |
|--------------------|----------------|---------------|
| Access             | SQL Count      | SQL           |
| Run-Time Parameter | Operator       | Default Value |
| Period From        | >=             | NOW -1 DAY    |
| Period To          | <=             | NOW           |

## S-TAP Agent Upgrade Pre-Check

Before starting a GIM upgrade, you can check whether any of the database servers that host Linux-UNIX S-TAP agents need to be rebooted during the S-TAP upgrade. This check is for GIM upgrades only; it does not cover any other upgrade scenarios.

If the bundles were installed from the managed unit, run the report on the managed unit. If all clients are managed by the central manager (all GIM clients point to the central manager, which is best practice and the recommended setup), run the report from the central manager. The reboot status of GIM clients that point to a managed unit is not captured in a report that is run on the central manager. Verify that the GIM agent is installed on the database server before you run the report (relevant for upgrades from a non-GIM installation). (None of the other modules or bundles need to be installed). All database servers that are listed in the report will need reboot.

There are no run-time parameters. This reporting domain is system-only.

Columns: S-TAP Host, Installed by GIM, GIM Parameter Name, Live Update.

| Run-Time Parameter      | Operator | Default Value |
|-------------------------|----------|---------------|
| Refresh rate in seconds |          | 0             |

## S-TAP agent with WINSTAP\_CMD\_LINE parameter

Displays details of what values exist in the WINSTAP\_CMD\_LINE field for all Windows S-TAPs.

Windows only: This report is available only for Windows systems.

There are no run-time parameters.

Columns: S-TAP Host, WINSTAP\_CMD\_LINE Parameter Value.

| Domain                   | Based on Query           | Main Entity |
|--------------------------|--------------------------|-------------|
| Internal - not available | Internal - not available | GIM Clients |

## S-TAP Configuration Change History

This report is displayed only when an inspection engine is added or changed. It lists the S-TAP configuration changes; each inspection engine change appears on a separate row. Each row lists the S-TAP Host, DB Server Type, DB Port From, DB Port To, DB Client IP, DB Client Mask, and Timestamp for the change.

| Domain                   | Based on Query               | Main Entity   |
|--------------------------|------------------------------|---------------|
| Internal - not available | Configuration Change History | Not available |
| Run-Time Parameter       | Operator                     | Default Value |
| Period From              | >=                           | NOW -1 DAY    |
| Period To                | <=                           | NOW           |

## S-TAP Events

Use this report for information on the S-TAP (from SOFTWARE\_TAP\_EVENT table in internal database).

| Domain                   | Based on Query | Main Entity   |
|--------------------------|----------------|---------------|
| Internal - not available | S-TAP Events   | Not available |
| Run-Time Parameter       | Operator       | Default Value |
| event type               | LIKE           | %             |
| host type                | LIKE           | %             |
| Period From              | >=             | NOW -3 DAY    |
| Period To                | <=             | NOW           |

## S-TAP Info (Central Manager)

On a Central Manager, an additional report, S-TAP Info, is available. This report monitors S-TAPs of the entire environment. Upload this data using the Custom Table Builder.

S-TAP info is a predefined custom domain which contains the S-TAP Info entity and is not modifiable like the entitlement domain.

When defining a custom query, go to upload page and click Check/Repair to create the custom table in CUSTOM database, otherwise save query will not validate it. This table loads automatically from all remote sources. A user cannot select which remote sources are used - it pulls from all of them.

Based on this custom table and custom domain, there are two reports:

**Enterprise S-TAP View** shows, from the Central Manager, information on an active S-TAP on a collector and/or managed unit (If there are duplicates for the same S-TAP engine, one being active and one being inactive, then the report only uses the active).

**Detailed Enterprise S-TAP View** shows, from the Central Manager, information on all active and inactive S-TAPs on all collectors and/or managed units.

If the Enterprise S-TAP View and Detailed Enterprise S-TAP View look the same, it is because there only one S-TAP on one managed unit being displayed. The Detailed Enterprise S-TAP View would look different if there are more S-TAPs and more managed units involved.

There is an Alert: Inspection Engines and S-TAP that alerts once a day on any activity related to inspection engine and S-TAP configuration. See [Predefined Alerts](#).

## S-TAP Last Response

Pre-defined query and report are available, but not added to any panels.

The query/report displays All S-TAP Hosts and the last response (heartbeat) sent by each host.

The purpose of this query is to be able to define an alert that triggers when an S-TAP on a host did not respond for a given period of time.

The input parameters are: Last response From, and, Last Response To.

For example, when executed with Last response From = NOW -5 DAYS and Last Response To = NOW - 3 HOURS, it displays the host name and the last response time for those hosts that sent the last response in the last 5 days, but had no response in the last 3 hours.

## S-TAP Status

Displays status information about each inspection engine defined on each S-TAP Host. This report has no From and To date parameters, since it is reporting current status. Each row of the report lists all the Guardium Hosts, DB Exec File, DB Server Type, Status, Last Response, Primary Host Name, Yes/No indicators for the following attributes: KTAP Installed, Shared Memory Driver Installed, DB2 Shared Memory Driver Installed, Named Pipes Driver Installed, and App Server Installed. In addition, it lists the Hunter DBS.

Note: The DB2 shared memory driver has been superseded by the DB2 Tap feature.

| Domain                   | Based on Query | Main Entity   |
|--------------------------|----------------|---------------|
| Internal - not available | S-TAP Status   | Not available |

## S-TAP Status Monitor

For each S-TAP reporting to this Guardium appliance, this report identifies the S-TAP Host, S-TAP Version, DB Server Type, Status (active or inactive), Last Response Received (date and time), Primary Host Name, and true/false indicators for: KTAP, MS SQL Server Shared Memory, DB2 Shared Memory, Local TCP monitoring, Named Pipes Usage, and Encryption; and the Guardium Hosts column that lists all hosts.

This report has no run-time parameters, and is based on a system-only query that cannot be modified.

## S-TAP Uninstall Events

Uninstalling an S-TAP could be evidence of harmful activity. This report details S-TAP uninstall events.

| Domain                   | Based on Query                   | Main Entity    |
|--------------------------|----------------------------------|----------------|
| Internal - not available | Not available                    | Not available  |
| Run-Time Parameter       | Operator                         | Default Value  |
| Period From              | >=                               | NOW -3 HOUR    |
| Period To                | <=                               | NOW            |
| Show Aliases             | Radio buttons (On, Off, Default) | Default        |
| Remote Data Source       |                                  | Drop-down menu |
| Refresh rate in seconds  |                                  | 0              |

## S-TAP Verification

List all results of S-TAP verifications, including: DB server type, Inspection engine identifier, Port range, Last response from S-TAP, Inspection engine status, Last verification time, Verification schedules, Next scheduled time, Datasource name, Datasource description, Verification type, Instance name, KTAP, MSS shm, WinDb2 shm, Win TCP, Pipes, Encrypted?, Firewall installed, DB install dir, Load balancing, Alternate IPs, TLS, DB Exec File.

| Domain                   | Based on Query     | Main Entity               |
|--------------------------|--------------------|---------------------------|
| Internal - not available | S-TAP Verification | S-TAP Verification Header |
| Run-Time Parameter       | Operator           | Default Value             |
| Query from date          | >=                 | NOW -3 HOUR               |
| Query to date            | >=                 | NOW                       |

## STAP/Z Files

STAP/Z provides files with raw data collected from DB2 (on z/OS®) containing DB2 events, SQL statements, etc. This report lists an Interface ID, UA file name (Un-normalized Audit Event), UT file name (Un-normalized Audit Event text), UH file name (Un-normalized Audit Event host variables), File Status, Total Number of Events Processed, Number of Events Failed, and Timestamp. The Run-time parameters are FileName Like % and FileStatus Like %.

This report has two run-time parameters, FileName Like % and FileStatus Like %. It is based on a system-only query that cannot be modified.

## Symptoms

| Domain                  | Based on Query                   | Main Entity    |
|-------------------------|----------------------------------|----------------|
| Eagle Eye               | Symptoms                         | Syptompe       |
| Run-Time Parameter      | Operator                         | Default Value  |
| Period From             | >=                               | NOW -3 HOUR    |
| Period To               | <=                               | NOW            |
| Enter Value for Case ID | Like                             | %              |
| Show Aliases            | Radio buttons (On, Off, Default) | Default        |
| Remote Data Source      |                                  | Drop-down menu |
| Refresh rate in seconds |                                  | 0              |

## TCP Exceptions

For the reporting period, for each exception where the Exception Description of the Exception Type entity is TCP/IP Protocol Exception, a row of this report lists the following attribute values from the Exception entity: Exception Timestamp, Exception Description, Source Address, Destination Address, Source Port, Destination Port, and count of Exceptions for that row.

| Domain             | Based on Query | Main Entity   |
|--------------------|----------------|---------------|
| Exceptions         | TCP Exceptions | Exception     |
| Run-Time Parameter | Operator       | Default Value |
| Period From        | >=             | NOW -1 DAY    |
| Period To          | <=             | NOW           |

## Templates (CAS)

This report lists CAS templates. By default, all template items are listed.

| Domain             | Based on Query | Main Entity   |
|--------------------|----------------|---------------|
| CAS Templates      | CAS Templates  | Template      |
| Run-Time Parameter | Operator       | Default Value |
| Access_Name        | Like           | %             |
| Template_Set_Name  | Like           | %             |
| Audit_Type         | Like           | %             |

## Test Detail Exception

This report lists all the test detail exceptions that are applied to a security assessment.

| Domain                   | Based on Query         | Main Entity   |
|--------------------------|------------------------|---------------|
| Internal - not available | Test Detail Exceptions | Not available |
| Run-Time Parameter       | Operator               | Default Value |
| Period From              | >=                     | NOW -3 HOUR   |
| Period To                | <=                     | NOW           |
| Approver                 | LIKE                   | %             |
| Exception Type           | LIKE                   | %             |
| Exception Detail         | LIKE                   | %             |
| Test Description         | LIKE                   | %             |
| Datasource Group         | LIKE                   | %             |
| Datasource Name          | LIKE                   | %             |
| Assessment               | LIKE                   | %             |
| Refresh Rate in seconds  |                        | 0             |

## Test Exceptions Original report and Test Exceptions report

Both reports indicate pairs of tests and datasources that are exempted temporarily. The Test Exceptions report is a more comprehensive version of the Test exceptions Original report.

### Test Exceptions Original report

Use the following selections to configure the Test Exceptions Original report:

| Domain                   | Based on Query  | Main Entity   |
|--------------------------|-----------------|---------------|
| Internal - not available | Test Exceptions | Not available |

| Run-Time Parameter | Operator | Default Value |
|--------------------|----------|---------------|
| Period From        | >=       | NOW -12 MONTH |
| Period To          | <=       | NOW           |

#### Test Exceptions report

Use the following selections to configure the Test Exceptions report:

| Domain                   | Based on Query  | Main Entity   |
|--------------------------|-----------------|---------------|
| Internal - not available | Test Exceptions | Not available |
| Run-Time Parameter       | Operator        | Default Value |
| Period From              | >=              | NOW -3 HOUR   |
| Period To                | <=              | NOW           |
| Approver                 | LIKE            | %             |
| Test Description         | LIKE            | %             |
| Datasource Group         | LIKE            | %             |
| Datasource Name          | LIKE            | %             |
| Assessment               | LIKE            | %             |
| Refresh Rate in seconds  |                 | 0             |

## Threat analytics case for analysis

When a case is assigned in the active threat analytics page, this report is sent to the assignee. It includes the case details and its observations.

| Domain                  | Based on Query                     | Main Entity               |
|-------------------------|------------------------------------|---------------------------|
| Active Threat Analytics | Threat analytics case for analysis | Analytic case observation |
| Run-Time Parameter      | Operator                           | Default Value             |
| Case number             | =                                  |                           |
| Period From             | >=                                 | NOW -3 HOURS              |
| Period To               | <=                                 | NOW                       |

## Threat Analytics Case Observations

This is a drill down report from the open cases and the closed cases reports. It shows the case's observations.

| Domain                  | Based on Query                     | Main Entity               |
|-------------------------|------------------------------------|---------------------------|
| Active Threat Analytics | Threat analytics case observations | Analytic case observation |
| Run-Time Parameter      | Operator                           | Default Value             |
| Case number             | =                                  |                           |
| Period From             | >=                                 | NOW -3 HOURS              |
| Period To               | <=                                 | NOW                       |

## Threat analytics closed cases

| Domain                  | Based on Query                | Main Entity   |
|-------------------------|-------------------------------|---------------|
| Active Threat Analytics | Threat analytics closed cases | Analytic case |
| Run-Time Parameter      | Operator                      | Default Value |
| Period From             | >=                            | NOW -3 HOURS  |
| Period To               | <=                            | NOW           |

## Threat analytics open cases

| Domain                  | Based on Query              | Main Entity   |
|-------------------------|-----------------------------|---------------|
| Active Threat Analytics | Threat analytics open cases | Analytic case |
| Run-Time Parameter      | Operator                    | Default Value |
| Period From             | >=                          | NOW -3 HOURS  |
| Period To               | <=                          | NOW           |

## Threat finder run log

This report gives results of the threat finder runs.

| Domain                   | Based on Query        | Main Entity                      |
|--------------------------|-----------------------|----------------------------------|
| Analytic Outliers Status | Threat Finder Run Log | Analytic status                  |
| Run-Time Parameter       | Operator              | Default Value                    |
| Period From              | >=                    | NOW -3 HOURS                     |
| Period To                | <=                    | NOW                              |
| Show Aliases             |                       | Radio buttons (On, Off, Default) |
| Remote Data Source       |                       | Drop-down menu                   |
| Refresh rate in seconds  |                       | 0                                |

## Throughput

For each Access Period in the reporting period, each row lists the Period Start time, the count of Server IP addresses, and the total number of accesses (Access Period entities).

You can restrict the output of this report using the Server IP run time parameter, which by default is set to % to select all IP addresses.

| Domain                   | Based on Query       | Main Entity   |
|--------------------------|----------------------|---------------|
| Internal - not available | DB Server Throughput | Not available |
| Run-Time Parameter       | Operator             | Default Value |
| Period From              | >=                   | NOW -1 DAY    |
| Period To                | <=                   | NOW           |
| Server IP                | LIKE                 | %             |

## Throughput (graphical)

This report is a Distributed Label Line chart version of the tabular Throughput report. It plots the total number of accesses over the reporting period, one data point per Period Start time.

You can restrict the output of this report using the Server IP run time parameter, which by default is set to % to select all IP addresses.

| Domain             | Based on Query               | Main Entity   |
|--------------------|------------------------------|---------------|
| Access             | DB Server Throughput - Chart | Access Period |
| Run-Time Parameter | Operator                     | Default Value |
| Period From        | >=                           | NOW -1 DAY    |
| Period To          | <=                           | NOW           |
| Server IP          | LIKE                         | %             |

## User Activity Audit Trail Reports

The User Activity Audit Trail menu selection displays two reports. In addition, from each of those reports, a third report can be produced. See:

- User Activity Audit Trail
- System/Security Activities
- Detailed Guardium User Activity (Drill-Down)

### User Activity Audit Trail

For the reporting period, for each User Name seen on a Guardium User Activity Audit entity, each row displays the Guardium User Name, an Activity Type Description (from the Guardium Activity Types entity), a Count of Modified Entity values, the Host Name, and the total number of Guardium Activity Audits entities for that row.

From any row of the this report, the Detailed Guardium User Activity report is available as a drill-down report.

| Domain             | Based on Query            | Main Entity                  |
|--------------------|---------------------------|------------------------------|
| Guardium Activity  | User Activity Audit Trail | Guardium User Activity Audit |
| Run-Time Parameter | Operator                  | Default Value                |
| Host Name          | LIKE                      | %                            |
| Period From        | >=                        | NOW -1 DAY                   |
| Period To          | <=                        | NOW                          |

### System/Security Activities

For the reporting period, for each User Name seen on a Guardium User Activity Audit entity, each row displays the Guardium User Name, an Activity Type Description (from the Guardium Activity Types entity), a Count of Modified Entity values, the Host Name, and the total number of Guardium Activity Audits entities for that row.

From any row of the this report, the Detailed Guardium User Activity report is available as a drill-down report.

| Domain             | Based on Query            | Main Entity                  |
|--------------------|---------------------------|------------------------------|
| Guardium Activity  | User Activity Audit Trail | Guardium User Activity Audit |
| Run-Time Parameter | Operator                  | Default Value                |
| Host Name          | LIKE                      | %                            |
| Period From        | >=                        | NOW -1 DAY                   |
| Period To          | <=                        | NOW                          |

### Detailed Guardium User Activity (Drill-Down)

This report is not available from the menu, but can be opened for any row of the User Activity Audit Trail report, or the System/Security Activities report. For the selected row of the report, based on the User Name and Activity Type Description, this report lists the following attribute values, all of which are from the Guardium User Activity Audit entity, except for the Activity Type Description, which is from the Guardium Activity Types entity: User Name, Timestamp, Modified Entity, Object Description, All Values, and a count of Guardium User Activity Audits entities for the row.

| Domain                    | Based on Query                  | Main Entity                  |
|---------------------------|---------------------------------|------------------------------|
| Guardium Activity         | Detailed Guardium User Activity | Guardium User Activity Audit |
| Run-Time Parameter        | Operator                        | Default Value                |
| Activity Type Description |                                 | value from calling report    |
| Period From               | >=                              | NOW -1 DAY                   |
| Period To                 | <=                              | NOW                          |
| User Name                 |                                 | value from calling report    |

Warning: Users should be aware that activities of the root user, and other sensitive system accounts, are logged. Drilling down into the activity of these users may show sensitive commands and passwords that have been entered on the command line. Therefore users, whenever possible, should not enter sensitive command line information that they would not like to show on this drill-down report.

## User Comments - Sharable

Sharable user comments are all comments except for inspection engine, installed policy, and audit process results comments. For each sharable user comment, this report lists the date created, the type of object referenced (an alert, for example), the object description, the user who created the comment, and the contents of the comment.

Note: Comments defined for inspection engines, installed policies, or audit process results can be viewed from the individual definitions, but they cannot be displayed on a report.

| Domain             | Based on Query   | Main Entity   |
|--------------------|------------------|---------------|
| Comments           | Comments Defined | Comments      |
| Run-Time Parameter | Operator         | Default Value |
| Period From        | >=               | NOW -2 MONTH  |
| Period To          | <=               | NOW           |

## User To-Do Lists

Displays for each Guardium audit process: a description, login name, action required (review or approve), status, user who has signed or reviewed, and execution date of the specified task.

| Domain                   | Based on Query   | Main Entity   |
|--------------------------|------------------|---------------|
| Internal - not available | Users To-do List | Not available |
| Run-Time Parameter       | Operator         | Default Value |
| Period From              | >=               | NOW -1 DAY    |
| Period To                | <=               | NOW           |

## Unit Utilization Levels

The following default reports provide unit utilization data:

- Unit Utilization: Displays the maximum unit utilization level for each unit in the given timeframe. There is a drill-down that displays details for a unit across all periods within the timeframe of the report.
- Unit Utilization Distribution: Per-unit, this report displays the percent of periods in the report timeframe with utilization levels of low, medium, and high.
- Utilization Thresholds: This predefined report displays all low and high threshold values for all unit utilization parameters.
- Unit Utilization Daily Summary: Provides a daily summary of unit utilization data.

| Domain                   | Based on Query                | Main Entity             |
|--------------------------|-------------------------------|-------------------------|
| Internal - not available | Unit Utilization Distribution | Unit Utilization Levels |
| Run-Time Parameter       | Operator                      | Default Value           |
| Period From              | >=                            | NOW -24 HOUR            |
| Period To                | <=                            | NOW                     |

## Values Changed

For the reporting period, this report provides detailed information about monitored value changes. All attribute values displayed are from the Monitor Values entity. The query this report is based upon has a non-standard sorting sequence, as follows:

- Server IP
- DB Type
- Audit Timestamp
- Audit Table Name
- Audit Owner

The query this report is based upon has a number of run-time parameters, all of which use the LIKE operator and default to the value %, meaning all values will be selected.

For each monitored value selected, a row of the report lists the Timestamp, Server IP, DB Type, Service Name, Database Name, Audit Login Name, Audit Timestamp, Audit Table Name, Audit Owner, Audit Action, Audit Old Value, Audit New Value, SQL Text, Triggered ID, and a count of Change Columns entities for that row.

| Domain             | Based on Query | Main Entity     |
|--------------------|----------------|-----------------|
| Value Changed      | Values Changed | Changed Columns |
| Run-Time Parameter | Operator       | Default Value   |
| Audit Action       | LIKE           | %               |
| Audit Login Name   | LIKE           | %               |
| Audit Owner        | LIKE           | %               |
| Audit Table Name   | LIKE           | %               |
| DB Type            | LIKE           | %               |
| Period From        | >=             | NOW -1 DAY      |
| Period To          | <=             | NOW             |
| Server IP          | LIKE           | %               |

## Predefined user reports

This section provides a short description of all predefined reports for users with default user access.

Note: If data level security at the observed data level is enabled (see [Data level security filtering](#)), then the audit process output is filtered so users see only the information about their databases.

### Active Users Last Login

Last login recorded during the reporting period for each member of the Active Users group. All members of the group will be listed, even if there were no logins during the reporting period. This is unlike most other reports based on members of a group. In the "normal" case, if no activity is found for a member, that member is not listed.

Each row lists a DB User Name, Client IP, Server IP, Server Type, Source Program, last login time (the maximum value of the Session Start attribute), and the count of sessions for the row.

The Active Users group is empty at installation time. It must be populated by someone at your location. The query that this report is based upon, Active Users Last Logins, cannot be accessed from the Query-Report Builder.

### Active Users with no Activity

Listing of members in the Active Users group who have had no activity during the reporting period. This report will be empty if all users have had activity during the reporting period.

The Active Users group is pre-defined, but empty at installation time. It must be populated by someone at your location. The query that this report is based upon, Active Users with no Activity, cannot be accessed from Query-Report Builder.

### Activity By Client IP

For each Client IP address seen during the reporting period, a row counts the number of SQL Verbs, Object Names, and the total number of sessions.

### Administrative Commands Usage

For each SQL Verb included in the Administrative Commands group that was seen during the reporting period, this report lists the SQL Verb, Depth, Object Name, and Client IP, and a count of objects referenced.

### Administrative Objects Usage

For each Object Name included in the Administration Objects group that was seen during the reporting period, each row lists the Object Name, Client IP, Server IP, Service Name, Database Name, Source Program, DB User Name, and Count of Objects for that row.

### Admin Users Login

For each DB User Name included in the Admin Users group, who had one or more sessions during the reporting period, each row lists the Client IP, DB User Name, Source Program, Session Start time, and Count of Sessions for that row.

### ALTER Commands Execution

All ALTER commands issued. The report displays the client IP from which the DDL was requested, server IP address, service name, database user name, source program, database name, object name, and main SQL verb (a specific DDL command) for each combination of client IP/DDL command listed on that specific line.

For each SQL Verb from the ALTER Commands group seen during the reporting period, this report displays the Client IP, Server IP, Service Name, DB User Name, Source Program, Database Name, Object Name, SQL Verb, and Count of Objects referenced in the row.

### Archive Candidates

This report lists objects (database tables or stored procedures, for example) that have not been accessed for an extended period of time. You cannot access the query this report is based upon.

### BACKUP Commands Execution

For each SQL Verb from the BACKUP Commands group seen during the reporting period, this report displays the Client IP, Server IP, Service Name, DB User Name, Source Program, Database Name, Object Name, SQL Verb, and Count of Objects referenced in the row.

### Classification Process Results

Lists classification process tasks.

### Client IP Activity Summary

This report displays reporting period activity from a single Client IP address, which is specified as a run time parameter. Each row of the report displays the Client IP, Source Program, SQL Verb, Depth (of sentence within the SQL command), an Object Name, and a count of times that object was referenced for that row.

## Commands List

This report lists all SQL Verbs seen during the reporting period. At the outermost level, commands are grouped by the Period Start time from the Access Period entity, which is usually one hour, on the hour. Your Guardium administrator can modify the access period length by changing the logging granularity, which is one hour by default. For each Access Period in the reporting period, each row lists the access Period Start time, a SQL Verb, Depth of the verb in the SQL statement, Parent (a pointer to the owning verb), and a count of occurrences for the row.

## Cosmos Full SQL

For the Azure Cosmos database, the Diagnostics setting includes DataPlaneRequests and a QueryRuntimeStatistics log that you can stream to an event hub.

For DataPlaneRequests, data is mapped between Cosmos and Guardium as follows:

- activityId maps to FULL SQL"."More Information"
- clientIpAddress maps to Guardium "Client/Server"."Client IP"
- database account is extracted from resourceId and maps to "Client/Server"."Server Host Name"
- duration maps to "FULL SQL"."RESPONSE\_TIME"
- operationName, requestResourceId, requestResourceType, resourceTokenPermissionId, responseLength, and statusCode are concatenated and mapped to "FULL SQL"."Full Sql"
- region is mapped to "Client/Server"."Server Description"
- time is mapped to "FULL SQL"."Timestamp"
- userAgent is mapped to "Client/Server"."Source Program"

For QueryRuntimeStatistics, data is mapped as follows:

- database account is extracted from resourceId and maps to "Client/Server"."Server Host Name"
- time maps to "FULL SQL"."Timestamp"
- databasename, collectionname, and querytext are concatenated and maps to "FULL SQL"."Full Sql"
- activityId and maps to "FULL SQL"."More Information"

When LOG\_FULL\_DETAILS action is selected, DataPlaneRequests and QueryRuntimeStatistics are saved as separate "FULL SQL" records, and the Cosmos Full SQL report correlates QueryRuntimeStatistics "FULL SQL" records to corresponding DataPlaneRequests "FULL SQL" records with the same activityId and then concatenates them both as "FULL SQL"."Full Sql".

| Domain | Based on Query  | Main Entity |
|--------|-----------------|-------------|
| Access | Cosmos Full SQL | FULL SQL    |

## CREATE Commands Execution

For each SQL Verb from the CREATE Commands group seen during the reporting period, this report displays the Client IP, Server IP, Service Name, DB User Name, Source Program, Database Name, Object Name, SQL Verb, and Count of Objects referenced in the row.

## Databases Discovered

For the reporting period, for each Discovered Port entity where the DB Type attribute value is NOT LIKE Unknown, this report lists the Probe Timestamp, Server IP, Server Host Name, DB Type, Port, Port Type, and count of Discovered Ports for the row.

| Domain             | Based on Query       | Main Entity     |
|--------------------|----------------------|-----------------|
| Auto-discovery     | Databases Discovered | Discovered Port |
| Run-Time Parameter | Operator             | Default Value   |
| Period From        | >=                   | NOW -1 DAY      |
| Period To          | <=                   | NOW             |

## Database Servers

For each Server IP address accessed during the reporting period, a row of the report displays the Server Type, Database Name, Service Name, a count of source programs accessing that server, and the total number of sessions for that row.

## Data Set z/OS Sensitive Object Activity

Displays all access to data sets in group z/OS Data Set Sensitive Objects.

| Domain             | Based on Query                | Main Entity   |
|--------------------|-------------------------------|---------------|
| Access             | DSz Sensitive Object Activity | FULL SQL      |
| Run-Time Parameter | Operator                      | Default Value |
| Period From        | >=                            | NOW -3 HOUR   |
| Period To          | <=                            | NOW           |
| pgm                | LIKE                          | %             |
| likeDSname         | LIKE                          | %             |

## Data Set z/OS Privileged User Activity

Displays all access by users in group z/OS Data Set Privileged Users.

| Domain | Based on Query               | Main Entity |
|--------|------------------------------|-------------|
| Access | DSz Privileged User Activity | FULL SQL    |

| Domain             | Based on Query               |               | Main Entity |
|--------------------|------------------------------|---------------|-------------|
| Access             | DSz Privileged User Activity |               | FULL SQL    |
| Run-Time Parameter | Operator                     | Default Value |             |
| Period From        | >=                           | NOW -3 HOUR   |             |
| Period To          | <=                           | NOW           |             |
| pgm                | LIKE                         | %             |             |
| likeDSname         | LIKE                         | %             |             |

## Data Sources

This report appears on the default layout for both administrators and users. See Data Sources on the Predefined Reports - Common page.

## Data Source Version History

This report appears on the default layout for both administrators and users. See Data Source Version History on the Predefined Reports - Common page.

## DB Predefined Users Login

For each DB User Name included in the DB Predefined Users group, who had one or more sessions during the reporting period, each row lists the DB User Name, Client IP, Server IP, Source Program, Database Name, Service Name, and Count of Sessions for that row.

## DBCC Commands Execution

For each SQL Verb from the DBCC Commands group seen during the reporting period, this report displays the Client IP, Server IP, Service Name, DB User Name, Source Program, Database Name, SQL statement, and Count of Objects referenced in the row.

## Db2 z/OS Sensitive Object Activity

Displays all access to tables in group z/OS DB2 Sensitive Objects for Reports.

| Domain             | Based on Query                 |               | Main Entity |
|--------------------|--------------------------------|---------------|-------------|
| Access             | Db2z Sensitive Object Activity |               | FULL SQL    |
| Run-Time Parameter | Operator                       | Default Value |             |
| Period From        | >=                             | NOW -3 HOUR   |             |
| Period To          | <=                             | NOW           |             |

## Db2 z/OS Privileged User Activity

Displays all access by users in group z/OS DB2 Privileged Users.

| Domain             | Based on Query                |               | Main Entity |
|--------------------|-------------------------------|---------------|-------------|
| Access             | Db2z Privileged User Activity |               | FULL SQL    |
| Run-Time Parameter | Operator                      | Default Value |             |
| Period From        | >=                            | NOW -3 HOUR   |             |
| Period To          | <=                            | NOW           |             |
| FullSQLLike        | LIKE                          | %             |             |
| Db2Subsystem       | LIKE                          | %             |             |
| NetwrkProtocol     | LIKE                          | %             |             |
| DbUser             | LIKE                          | %             |             |

## DDL Commands

All DDL commands sent to the database. The report displays the client IP from which the DDL was requested, the main SQL verb (a specific DDL command), and the total objects accessed for that record.

For each SQL Verb from the DDL Commands group seen during the reporting period, this report displays the Client IP, Server IP, Server Type, SQL Verb, and Count of Commands referenced in the row.

## DDL Distribution

This bar graph displays the distribution of commands seen from the DDL Commands group during the reporting period. For each command seen, a single bar represents the total number of objects affected.

## DML Execution on Administrative Objects

For each SQL Verb from the DML Commands group that references an Object Name in the Administration Objects group, this report displays a row for the DB User Name, Client IP, Server IP, Server Type, Service Name, Database Name, SQL Verb, Object Name, and Count of Objects referenced in the row.

## DML Execution on Sensitive Objects

For each SQL Verb from the DML Commands group that references an Object Name in the Sensitive Objects group, this report displays a row for each Access Period, Client IP, and Source Program, with a total count of objects referenced in that row. Although the report title contains the word Executions, there is no guarantee that all commands reported were actually executed.

## DROP Commands Execution

---

For each SQL Verb from the DROP Commands group seen during the reporting period, this report displays the Client IP, Server IP, Service Name, DB User Name, Source Program, Database Name, Object Name, SQL Verb, and Count of Objects referenced in the row.

## DW Dormant Objects

---

Shows all the members of one group that are not members in a second group, with a focus on dormant tables. For example, this report shows objects that are in the all objects group, but have not been used in a Select.

## DW Dormant Objects/Fields

---

Shows all the members of one group that are not members in a second group, with a focus on dormant tables and columns. In this instance, groups are a 2-tuple type (members that are a composite of a pair of value attributes). For example, this report shows objects that are in the all objects and fields group, but have not been used in a Select.

## DW EXECUTE Object Access

---

Use this report to populate the group called DW EXECUTE Objects with a set of stored procedure names that being executed. Then use indirect mapping in Group Builder/Auto Generate Calling Prox to generate all the objects being used within these procedures.

## DW SELECT Object Access

---

This report shows all object names that have been accessed through a SELECT statement.

## DW SELECT Object-Field Access

---

This report shows all object and field names that have been accessed through a SELECT statement.

## Exception Count

---

The total number of exceptions (Exception entities) logged during the reporting period.

## Exceptions Distribution

---

Each wedge of the pie chart represents the proportion of exceptions for each Exception Description attribute value (from the Exception Type entity) that was logged during the reporting period.

As with any chart, you can drill down on the pie chart to display the tabular version of the query on which the chart is based. There are several exceptions reports that are accessible from this tabular report (or drill-downs from it) that are available here, but are not included on any menu.

## Exceptions Monitor

---

A count of exceptions logged during the reporting period. One datapoint is created each time that you refresh the report on your portal.

## Excessive Errors per period

---

Display #Errors/Period; E.g., more than N errors in 60min for the same Client IP address, Server IP address, Server Type, database user name.

## Failed User Login Attempts

---

For each failed login attempt during the reporting period, lists the User Name, Source Address, Destination Address, and Database Protocol Type for the server the user was attempting to log into.

## Flat LOG List

---

Lists flat log processing tasks.

## Full SQL By Client IP

---

This report displays reporting period Full SQL attribute values that have been logged for a single Client IP, which is specified as a run time parameter. Each row of the report displays the Full SQL ID, Timestamp (of the Full SQL entity), Client IP, DB User Name, Session Start, Source Program, Full SQL, and a count of occurrences for the row.

## Full SQL By DB User Name

---

This report displays reporting period Full SQL attribute values that have been logged for a single DB User Name, which is specified as a run time parameter. Each row of the report displays the Full SQL ID, Timestamp (of the Full SQL entity), Client IP, DB User Name, Session Start, Source Program, Full SQL, and a count of occurrences for the row.

## GRANT Commands Execution

---

For each SQL Verb from the GRANT Commands group seen during the reporting period, this report displays the Client IP, Server IP, Service Name, DB User Name, Source Program, Database Name, Object Name, SQL Verb, and Count of Objects referenced in the row.

## Guardium Job Queue

---

Displays the Guardium Job Queue. For each job, lists the Process Run ID, Process Type, Status, Cls/Asmt Process Id, Report Result Id, Cls/Asmt Description, Audit Task Description, Queue Time, Start Time, End Time, and Data Sources.

| Domain                   | Based on Query     | Main Entity   |
|--------------------------|--------------------|---------------|
| internal - not available | Guardium Job Queue | not available |
| Run-Time Parameter       | Operator           | Default Value |
| Job Description          | LIKE               | %             |
| Period From              | >=                 | NOW -1 DAY    |
| Period To                | <=                 | NOW           |

## Hourly Access Details

---

This report produces a highly detailed listing for each DB User Name seen in the reporting period, which is one hour by default for this report. Each row of the report lists a DB User Name, Client IP, Server IP, Period Start, Source Program, SQL (from the SQL entity), and a count of occurrences during the access period.

## IMS Access (z/OS)

---

Use this to report to view details of access to the IMS (z/OS®).

| Domain             | Based on Query | Main Entity   |
|--------------------|----------------|---------------|
| Access             | IMS Access     | Client Server |
| Run-Time Parameter | Operator       | Default Value |
| Period From        | >=             | NOW -2 HOUR   |
| Period To          | <=             | NOW           |

## IMS Object (z/OS)

---

Use this to report to view an object-level view of access to the IMS (z/OS).

| Domain             | Based on Query | Main Entity   |
|--------------------|----------------|---------------|
| Access             | IMS Object     | Object        |
| Run-Time Parameter | Operator       | Default Value |
| Period From        | >=             | NOW -2 HOUR   |
| Period To          | <=             | NOW           |

## IMS Event (z/OS)

---

Use this to report for a summary of the type of access (such as DLI), and the command and object mapping of IMS (z/OS) events.

| Domain             | Based on Query | Main Entity   |
|--------------------|----------------|---------------|
| Access             | IMS Event      | SQL           |
| Run-Time Parameter | Operator       | Default Value |
| Period From        | >=             | NOW -2 HOUR   |
| Period To          | <=             | NOW           |

## IMS Data Access Details (z/OS)

---

This report uses the Full SQL Entity as the main entity and provides full details of each access to the IMS (z/OS).

| Domain             | Based on Query          | Main Entity   |
|--------------------|-------------------------|---------------|
| Access             | IMS Data Access Details | Full SQL      |
| Run-Time Parameter | Operator                | Default Value |
| Period From        | >=                      | NOW -2 HOUR   |
| Period To          | <=                      | NOW           |
| Client IP          | LIKE                    |               |
| DBUserName         | LIKE                    |               |
| IMS Name           | LIKE                    |               |
| ServerIP           | LIKE                    |               |

## IMS z/OS - Privileged User Activity

Displays all access by users in group z/OS IMS Privileged Users for Reports.

| Domain             | Based on Query                |               | Main Entity |
|--------------------|-------------------------------|---------------|-------------|
| Access             | IMSz Privileged User Activity |               | FULL SQL    |
| Run-Time Parameter | Operator                      | Default Value |             |
| Period From        | >=                            | NOW -3 HOUR   |             |
| Period To          | <=                            | NOW           |             |
| ServiceName        | LIKE                          | %             |             |
| IMSUserID          | LIKE                          | %             |             |
| FullSQL            | LIKE                          | %             |             |

## IMS z/OS - Sensitive Object Activity

Displays all access to segments in group z/OS IMS Sensitive Objects for Reports.

| Domain             | Based on Query                 |               | Main Entity |
|--------------------|--------------------------------|---------------|-------------|
| Access             | IMSz Sensitive Object Activity |               | FULL SQL    |
| Run-Time Parameter | Operator                       | Default Value |             |
| Period From        | >=                             | NOW -3 HOUR   |             |
| Period To          | <=                             | NOW           |             |
| ServiceName        | LIKE                           | %             |             |
| IMSUserID          | LIKE                           | %             |             |
| FullSQL            | LIKE                           | %             |             |
| IMSDBD             | LIKE                           | %             |             |

## KILL Commands Execution

For each SQL Verb from the KILL Commands group seen during the reporting period, this report displays the Client IP, Server IP, Service Name, DB User Name, Source Program, Database Name, Object Name, SQL Verb, and Count of Objects referenced in the row.

## Logged R/T Alerts

This report displays a bar representing the total number of alerts logged during the reporting period, for each type of real-time alert logged, based on the Access Rule Description attribute of the Policy Rule Violation entity.

## Logged Threshold Alerts

This report displays a bar representing the total number of alerts logged during the reporting period, for each type of threshold alert logged, based on the Alert Description attribute of the Threshold Alert Details entity.

## Long Running Queries

For the reporting period, this report lists the longest running queries, with the longest average execution time first. For each query, lists the Client IP, Server IP, SQL, Period Start (from the Access Period entity), Average Execution Time, and the count of occurrences for this row. You cannot access the query this report is based upon.

## Number of Active Privacy Set Tasks

Number of active Guardium audit processes that contain one or more privacy set tasks. When central management is used, this report contains data on the Central Manager only, and is empty on all managed units (the standard message, No data found for requested query, displays). This report has non-standard run time parameters: there are no from and to date parameters, so all audit processes containing one or more privacy set tasks will be reported. You can clone the query that this report is based upon (Number of Active Privacy Set Processes), but you cannot clone or regenerate the default report. The cloned query will have all of the standard run-time parameters (including the from and to dates).

## Number of Active Audit Processes

The number of active Guardium audit processes. When central management is used, this report contains data on the Central Manager only, and is empty on all managed units (the standard message, No data found for requested query, displays). This report has non-standard run time parameters: there are no from and to date parameters, so all active audit processes will be reported. You can clone the query that this report is based upon (Number of Active Processes), but you cannot clone or regenerate the default report. The cloned query will have all of the standard run-time parameters (including the from and to dates).

## Number of db per type

Displays the number of servers and clients for each monitored database type (default time period is the current day).

## Object Activity Summary

This report displays reporting period activity for a single Object Name, which is specified as a run time parameter. Each row of the report displays the Client IP, Source Program, SQL Verb, Depth (of sentence within the SQL command), an Object Name, and a count of times that object was referenced for that row.

## Objects List

---

This report lists all objects seen during the reporting period. At the outermost level, objects are grouped by the Period Start time from the Access Period entity, which is usually one hour, on the hour. Your SQL Guard administrator can modify the access period length by changing the logging granularity, which is one hour by default. For each Access Period in the reporting period, each row lists the access Period Start time, an Object Name, and the count of occurrences for that row.

## One User One IP

---

For each DB User Name for which session data was collected during the reporting period, each line of this report displays the count of Client IP addresses from which the user logged in, and a total number of sessions.

## Outstanding Audit Process Reviews

---

For each Guardium user Login Name, this report lists the number and type of outstanding Guardium audit processes. An outstanding audit process has a Status attribute value (in the Task Results To-Do-List entity) other than Reviewed or Signed. This report has non-standard run time parameters: there are no from and to dates, which means that all outstanding task results will be reported. You can clone the query that this report is based upon (it has the same name), but you cannot clone or regenerate the default report. The cloned query will have all of the standard run-time parameters (including the from and to dates).

## Policy Violation Count

---

For the reporting period, this report displays the number of policy violations logged.

## Privileged Account Utilization

---

Show User, Verb, and the Count of Periods within which the Verb was performed by a User in the group Admin Users

## Privileged User Access of Business Objects

---

Show User, Verb, Object where the User in Admin Users and the Verb was performed by the on an Object that is in a selected group of Business Objects

## Policy Violations

---

For every policy rule violation logged during the reporting period, this report provides the Timestamp from the Policy Rule Violation entity, Access Rule Description, Client IP, Server IP, DB User Name, Full SQL String from the Policy Rule Violation entity, Severity Description, and a count of violations for that row. You cannot access the query that this report is based upon (Policy Violations List with Severity), but you can clone the report.

## Request Rate

---

By default, displays the request rate for the last two hours. This graphical report is intended to display recent activity only. If you alter the From and To run-time parameters to include a longer timeframe, you may receive a message indicating that there is too much data. (Use a tabular report to display a larger time period.)

## RESTORE Commands Execution

---

For each SQL Verb from the BACKUP Commands group seen during the reporting period, this report displays the Client IP, Server IP, Service Name, DB User Name, Source Program, Database Name, Object Name, SQL Verb, and Count of Objects referenced in the row.

## REVOKE Commands Execution

---

For each SQL Verb from the REVOKE Commands group seen during the reporting period, this report displays the Client IP, Server IP, Service Name, DB User Name, Source Program, Database Name, Object Name, SQL Verb, and Count of Objects referenced in the row.

## Sensitive Objects Usage

---

For each object in the Sensitive Objects group, displays a row for each Client IP and Source Program that referenced the object during the reporting period, and a count of object references.

The Sensitive Objects group is empty at installation time. Someone at your company must populate the group with the appropriate set of members.

## Sessions By Server Type

---

For each server type (DB2®, Informix®, etc.), a row of this report displays the total number of sessions that were open during the reporting period (by default, the last three hours).

## Sessions List

---

This report lists all database sessions for the reporting period. For each session, the report displays the session (entity) Timestamp, the Session Start (timestamp), Server Type, Client IP, Server IP, Client Port, Server Port, Network Protocol, DB Protocol, DB Protocol Version, DB User Name username, Source Program, and Count of Sessions for that row (which should always be 1).

As with most reports, drill-down reports are available. There are a number of session reports that are accessible from this report, but are not included on any menu. This includes the following reports, with the run time parameters for those reports set by using values from the selected row of the report:

| <b>Report</b>              | <b>Run-time Parameters</b> |
|----------------------------|----------------------------|
| Sessions by Client IP      | Server IP, Server Type     |
| Sessions by Server IP      | Server Type                |
| Sessions by Source Program | Server Type, Server IP     |
| Sessions by User           | Server Type, Server IP     |
| Sessions Details by Server | Server Type, Server IP     |

## SQL Errors

For each SQL error during the reporting period, displays the Client IP address, Server IP address, Server Type, database user name, database error text, and error occurrence total for that record.

## Terminated Users Failed Login Attempts

Lists failed login attempts by database users who are members of the Terminated DB User group. This report will be empty if there were no failed login attempts by anyone in this group during the reporting period.

The Terminated DB Users group is pre-defined, but empty at installation time. It must be populated by someone at your location. The built-in query for this report cannot be accessed. The query that this report is based upon (Terminated Users Failed Login Attempts) cannot be accessed from any query builder.

## Terminated Users Logins

Lists all logins by database users who are members of the Terminated DB User group. Each row lists a DB User Name, Client IP, Server IP, Server Type, Source Program, last login time (the maximum value of the Session Start attribute), and the count of sessions for the row.

The Terminated DB Users group is empty at installation time. It must be populated by someone at your location. The query that this report is based upon, Terminated Users Logins, cannot be accessed from the Query-Report Builder.

## Throughput

This report produces a count of all Server IPs seen, and total accesses, during the reporting period. At the outermost level, accesses are grouped by the Period Start time from the Access Period entity, which is usually one hour, on the hour. Your Guardium® administrator can modify the access period length by changing the logging granularity, which is one hour by default. Each row lists the Period Start time, the count of Server IPs seen, and a total count of accesses for the row.

You can restrict the output of this report using the Server IP run time parameter, which by default is set to "%" to select all IP addresses.

## Throughput (Graphical)

This report is a Distributed Label Line chart version of the tabular Throughput report, plotting the total number of accesses over the reporting period, one data point per Period Start time.

You can restrict the output of this report using the Server IP run time parameter, which by default is set to "%" to select all IP addresses.

## Users inactive since

Show User and Last Session Start for all users having Access records and having max Session Start time earlier than 90 days ago. (an inactive user is missed if they never once logged in, or if all their old logins have been purged)

## Violations/Incidents

See [Incident Management](#).

## View Installed Policy

In the Currently Installed Policy panel, this special report displays the information about the installed policy such as the policy name, the number of rules it contains, and its policy definition settings. You cannot access the query this report is based upon.

## Predefined common reports

This section provides a short description of all predefined reports available for users with either default user access rights or default admin access rights.

The common reports are:

- Data Source Version History
- Data Sources

## Status Monitor

The Status Monitor graphical report displays the current state of the guardium appliance: how many packets per second and requests per second it is processing, how much disk space and memory is being used, and so forth. Each field is described in the following table.

The box displays the output of the Linux® VMSTAT command. If you are familiar with that command, these statistics should be familiar to you.

| Field                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| procs                           | The number of processes:<br><br><b>r:</b> Waiting for run time.<br><br><b>b:</b> In uninterruptable sleep (blocked, waiting for another event).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| memory                          | Memory use (kB):<br><br><b>swpd:</b> Amount of virtual memory used.<br><br><b>free:</b> Amount of idle memory.<br><br><b>buff:</b> Amount used as buffers.<br><br><b>cache:</b> Amount reserved for cache.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| swap                            | Amount of memory (kB):<br><br><b>si:</b> Swapped in from disk.<br><br><b>so:</b> Swapped out to disk.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| io                              | Input/Output blocks (kB/s):<br><br><b>bi:</b> Blocks received from a block device<br><br><b>bo:</b> Blocks sent to a block device                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| system                          | System:<br><br><b>in:</b> Interrupts per second, including the clock<br><br><b>cs:</b> Context switches per second                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| cpu                             | Percentage of total CPU time used by:<br><br><b>us:</b> Time spent running non-kernel code<br><br><b>sy:</b> Time spent running kernel code<br><br><b>id:</b> Idle time (not including waiting for IO)<br><br><b>wa:</b> Time spent waiting for IO<br><br><b>st:</b> Time stolen from a virtual machine                                                                                                                                                                                                                                                                                                                                                                                                                         |
| (n)pps / (m)rps                 | In the arrow next to the Analysis Engine, two averages are calculated for the last five seconds: <b>n</b> is the average number of network packets per second, and <b>m</b> is the average number of network database requests per second.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Analysis Engine (q-d) ----- (p) | For the Analysis Engine, the first line lists the total number of messages queued for processing ( <b>q</b> ), followed by the number of messages dropped ( <b>d</b> ) because the buffer was in danger of becoming filled. The second line lists the total number of messages processed ( <b>p</b> ). The number processed will be reset to zero whenever the inspection engine is restarted.                                                                                                                                                                                                                                                                                                                                  |
| Server Type (q) ---- (p)        | For each server type, the number of messages awaiting processing ( <b>q</b> ) is listed and the number of messages processed ( <b>p</b> ) is listed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Free Disk Space                 | The number of bytes free.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| DB n% Full                      | The percentage of the database space allocation that is used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Files/Other                     | The Files/Other portion of Status Monitor represents the data accumulated in nondb-sql logger.<br>Nondb-sql logger logs close session events arriving to the Analyzer from "ignored" sessions that have been internally closed by the Analyzer (INACTIVE_FLAG=-1). The Analyzer has the ability to close connections by timeout (if session has been inactive for a long time). If close session data arrives to the Analyzer from "ignored" session that has been closed by timeout, it is recorded in the nondb-sql-logger section.<br><br>Analyzer never records data directly to database. This section also represents number of DB requests sent by Analyzer to Logger, as well as other supported protocols such as SCP. |

## Data Source Version History

Default Layout Location

- admin: available as drill-down from the Data Sources report
- user: Discover > DB Discovery

## Data Sources

Lists all datasources defined: Data -Source Type, Data-Source Name , Data-Source Description, Host, Port, Service Name, User Name, Database Name, Last Connect, Shared, and Connection Properties..

You can restrict the output of this report using the Data Source Name run time parameter, which by default is set to "%" to select all datasources.

| Domain                   | Based on Query | Main Entity   |
|--------------------------|----------------|---------------|
| internal - not available | Data-Sources   | not available |
| Run-Time Parameter       | Operator       | Default Value |
| Data Source Name         | LIKE           | %             |
| Period From              | >=             | NOW -1 DAY    |
| Period To                | <=             | NOW           |

## Predefined Audit Processes

---

There is one predefined audit process named Appliance Monitoring, which contains the proceeding reports listed. This audit process is inactive by default. The administrator can activate and schedule it according to his or her needs.

Note: When scheduling this audit process, check that the FROM/TO dates for each report make sense for the process interval being defined (for example, it doesn't make sense to have a reporting period of one day if the audit process runs only once a week - you will miss six days of activity).

The Appliance Monitoring audit process contains the following reports:

- Failed Logins to Guardium
- Active Guardium Users
- Aggregation/Archive Errors
- Policy Related Changes
- Inspection Engines and S-TAP Changes
- Data Source Changes
- CAS Instance Configuration Changes
- CAS Instances
- CAS Templates
- Scheduled Jobs Excep

---

## Creating dashboards and adding reports

You can create one or more dashboards, add reports to them, and configure their appearance.

### Before you begin

---

Think about how you want to organize the reports that you view regularly. Do you want to view them in one dashboard, or in several dashboards? Do you want to group and order them according to their purpose, how critical they are, or some other approach? You can always rearrange your dashboards or create new ones.

### Procedure

---

1. Click My Dashboards  Create New Dashboard to open a new dashboard.
2. Enter a descriptive name in the Name field. This name is used in the list of dashboards in the menu.
3. Click Add Report  to display a list of available reports. If you have designated certain reports as favorites, you can check the My Favorites box to see only a list of those reports. If you want to see only graphical reports, check the Chart Only box.  
The Add a Report dialog shows a list of all reports that meet your criteria. You can browse the list of reports, or type a string in the Filter field. The list of reports is updated as you type.
4. Click the title of a report to add it to your dashboard. Continue adding as many reports as you want. When you are finished adding reports, click Close.
5. Click Edit mode to add the toolbar to individual reports so you can modify the reports. (See [Viewing reports](#).)

### Results

---

You have a dashboard that gives you easy access to some selected reports.

### What to do next

---

Review the appearance of your dashboard. Is it easy to use, and to find the information that you want? If not, you can configure it further.

### Customize your dashboard

---

Learn how to customize your dashboard.

#### Procedure

1. Change the dashboard by clicking  and entering the new name.
2. Select the number of column in the upper right corner. The default is two columns.
3. Rearrange the reports. To move a report, place your cursor on the report's title bar, and drag it to a new location.
4. Resize your reports. Drag the resize icon to make a report longer or shorter, narrower or wider.
5. Designate specific reports as favorites by clicking  (in edit mode only).
6. Delete a dashboard by clicking Delete dashboard.

---

## Opening the investigation dashboard, filtered for report entities

### About this task

---

From tabular reports that include columns related to the investigation dashboard filter fields (for example: DB User, Server IP, Database, Source Program), you can open the investigation dashboard, filtered for those values.

## Procedure

Right-click the row of a report and select Investigate In Dashboard.

## Results

The investigation dashboard opens, filtered for the values in that row of the report. If the "from date" and "to date" run time parameters are defined, the dashboard uses the values. If they are not defined, the dashboard opens with "Last 1 Hour" time filter.

## Viewing reports

There are several ways to view a report, including your dashboard and UI search.

You can view a report in several ways:

- If you have saved the report to a dashboard, open the dashboard to view the report.
- You can add the report to a dashboard. Open the dashboard and click Add Report, then choose the report from the list.
- Add the report to your custom reports.
- Some reports are listed in categories in the Reports lifecycle.
- Some reports are listed under the lifecycle to which they are most relevant.
- You can use the user interface (UI) search function to find a report that is in a lifecycle or in a dashboard. On the banner, choose User Interface from the drop-down list next to the Search box. Enter the name of the report into the Search box. Results begin to appear after you type a few characters. Choose the report from the list of results.

After upgrading from pre-v10.6 to v10.6 and higher: If you had multiple reports based on the same query, upon upgrade there is one query for every report whose name is the same as the report in the pre-upgrade version.

The following choices (icons) give access to editing and configuring the report:

|  |                                                                                                                                                                                                                                                                                                          |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Edit the query for this report ( <a href="#">Using the Query-Report Builder</a> ).                                                                                                                                                                                                                       |
|  | Opens a new Query-report page with a copy of the report, except for the name. Modify and save as relevant. See <a href="#">Using the Query-Report Builder</a> .                                                                                                                                          |
|  | Opens the Data Mart Configuration dialog. For more information, see <a href="#">Data Mart</a> .                                                                                                                                                                                                          |
|  | <a href="#">Ad-hoc process for run once now</a>                                                                                                                                                                                                                                                          |
|  | Opens the report in a new window.                                                                                                                                                                                                                                                                        |
|  | <a href="#">Modifying the report display</a>                                                                                                                                                                                                                                                             |
|  | Configure report columns: add or remove columns.                                                                                                                                                                                                                                                         |
|  | Configure runtime parameters. A run-time parameter provides a value to be used in a query condition. There is a default set of run-time parameters for all query-reports, and any number of run-time parameters can be defined in the query-report. ( <a href="#">Modifying the runtime parameters</a> ) |
|  | Add to favorites                                                                                                                                                                                                                                                                                         |
|  | Stops generation of a report (relevant for reports that take a longer time to generate)                                                                                                                                                                                                                  |
|  | Refresh the report. See <a href="#">Refreshing reports</a>                                                                                                                                                                                                                                               |

You can hide columns from view. Click the columns icon and clear the check boxes for the columns that you want to hide.

You can sort report data by the contents of any column. Click the title of the column on which you want to sort. To reverse the order, click the title again. Sorting is always performed on the actual data values, ignoring any aliases that are defined.

You can print a report while you are viewing it. Click Export > Full printable report to open a printable copy of the report in a new tab. Click the printer icon on the new tab to print the report. You can also print a report by exporting it to a PDF file and printing the PDF file.

Note: For an instance where the PDF text is too small to read, the PDF report has a physical limit on how much it can expand horizontally given how wide the page is. Since each line of the PDF report has to fit on one line, the typeface size changes to fit the data, and may force a very small typeface size in order to display all the data. Graphical reports can be customized by clicking the Customize Chart icon. The choices include converting the data to a line chart, changing the X-axis and Y-axis orientation, converting the report to a pie chart or a stacked column chart.

When viewing reports that display Oracle information, occasionally the ? question mark character is used to inform the viewer that the login information was not available. Again when viewing reports that display Oracle information, the appearance of the number -1 signifies that an unknown number of records are affected. All Oracle sessions are recorded, even with missed logins.

The OS user does not appear in reports if a Linux system or a Windows system using remote connections did not send the OS user with the login packet. For Linux local connections, UID chain can be used to identify the user. See which systems support UID chains in [S-TAP support matrix](#).

Viewing Big Data Intelligence reports has a few differences.

- Reports present data in batches of 1000 items. Each page contains the number of rows defined in the lower right corner. The page numbers under the report show the page within the batch. Page through the batch using the page numbers. Proceed to the next batch with Next batch. You can move forward in the batches. Run the query again to view earlier batches.

Note: If you sort the report, either by clicking a column name or by setting the sort order in the query-report itself, you only see one batch.

- Clicking Refresh reruns the query.

- [Modifying the runtime parameters](#)

You can modify the runtime parameters to control the contents and presentation of a report.

- [Refreshing reports](#)

Some reports are configured to refresh their data automatically. On other reports, you can refresh the data manually through the UI.

- [Exporting a report](#)  
You can export a report to a PDF file or a comma-separated values file.
- [Viewing Drill-Down Reports](#)  
Many reports provide access to drill-down reports that provide more granular data.
- [Ad-hoc process for run once now](#)  
This process creates and runs an ad-hoc audit process report.

## Modifying the runtime parameters

You can modify the runtime parameters to control the contents and presentation of a report.

This table lists the standard runtime parameters. A report may have additional parameters.

| Runtime Parameter      | Default                                         | Description                                                                                                                                                                                                           |
|------------------------|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enter Period From      | NOW -3 HOUR.                                    | Required. Start time of the report. The default is NOW -3 HOUR. For Big Data intelligence, the default is NOW -1 DAY. Predefined reports may have different defaults.                                                 |
| Enter Period to        | NOW                                             | Required. End time of the report. The default is NOW. Predefined reports may have different defaults.                                                                                                                 |
| Guardium appliance     | All                                             | Big Data Intelligence only. Data is retrieved for all Guardium appliances (default) or the selected one.                                                                                                              |
| Time Zone              | The time zone of your Guardium system.          | Big Data Intelligence only. Data is retrieved according to this time zone and date fields are presented in this time zone.                                                                                            |
| Remote Data Source     | None                                            | In a Central Manager environment, you can run a report on a managed unit by selecting that Guardium system from the Remote Data Source list.                                                                          |
| Show Aliases           | None (meaning the system-wide default is used). | Select On to always display aliases, or Off to never display aliases. Select Both to display both the original and alias value. Select Default to revert to the system-wide default (controlled by the administrator) |
| Refresh Rate (seconds) | 0                                               | Rate at which the report is refreshed, in seconds. 0 means the report is not refreshed automatically.                                                                                                                 |

Use the GuardAPI command, `list_parameter_names_by_report_name`. This function takes a report name as an input parameter and returns a list of runtime parameter names for that report.

1. Access the report.
2. Click Configure runtime parameters .
3. Modify the parameters as relevant and click OK.

## Refreshing reports

Some reports are configured to refresh their data automatically. On other reports, you can refresh the data manually through the UI.

There are several ways to refresh report data manually:

- Click Refresh  on the report toolbar.
- Use any toolbar button to print a report, download report data, or write the report to a PDF file. The report data is refreshed before performing any of these actions.
- Set a time interval for periodic refreshing, by setting the `refreshRate` parameter value. To perform this task:
  - Click  on the report toolbar.
  - In the Configuration dialog, set the `refreshRate` parameter to the number of seconds after which the report data is to be updated. The default value of zero indicates that the report data is not refreshed on a scheduled basis.
  - Click OK.

## Exporting a report

You can export a report to a PDF file or a comma-separated values file.

You can export the contents of a report to:

- PDF. When you generate a large PDF file, the process can cause the UI to time out. If you plan to generate large PDF files, consider doing so as part of an audit process, or increasing the UI timeout value to avoid this problem.
- CSV of all records
- CSV of the display records (the data currently displayed)

Restriction: PDFs generated manually or using an audit process are limited to 5,000 rows. Manually exported CSV files are limited to 30,000 rows (this default is configurable using the `store csv_max_size` CLI command). Any number of rows can be exported to CSV when using an audit process.

1. Access the report.
2. Click Export in the toolbar, and select one of:
  - Download all records: CSV of all records. You can save and/or view the file.
  - Download display records: CSV of the display records (the data currently displayed). You can save and/or view the file.
  - Full printable report: Opens a new browser window with all the report details.
  - Download as PDF: You can save and/or view the file.

# Viewing Drill-Down Reports

Many reports provide access to drill-down reports that provide more granular data.

If any drill down actions are available on a tabular report, you can see them by right-clicking on a row of the grid. The context-menu appears with any available drill-down actions.

To be available as a drill-down report:

- All of the runtime parameters for the drill-down report must be available from the report that is being viewed.
- If security roles have been assigned, you must have access to the drill-down report.

## Related tasks

- [Modifying the query drilldown control](#)

## Ad-hoc process for run once now

This process creates and runs an ad-hoc audit process report.

## About this task

The behavior of this process is as follows:

1. If a new process, one or a number of email receivers can be created in the list (if any) with a content type as indicated in the emailContentType parameter. It also creates a user receiver for the user logged in (invoking the API) if the includeUserReceiver parameter is true.
2. If an existing process, all email receivers are removed and replaced with the emails from the new list (if any) with the content type as defined in the emailContentType parameter. If the list is empty, it removes all email address receivers. If there is already a receiver for the user it is NOT even if the includeUserreceiver is false, however if the parameter is true and there is no such receiver then it is added.

Once the audit process is generated it automatically executes (similar to a Run Once Now) and users should expect an item on their to-do list for that audit process. The GuardAPI that creates ad hoc audit process keeps results to 7 days (instead of 1 day). Results are deleted after 7 days. For further information on parameters, see the GuardAPI command, `create_ad_hoc_audit_and_run_once`, in the GuardAPI Input Generation help topic.

## Procedure

1. Click the Ad-hoc process for Run Once Now icon  .
2. In the Ad-hoc dialog, fill in as relevant, then click OK.
  - Email Addresses: comma separated list of email addresses.
  - Content type for email receiver: PDF or CSV (a radio button 0 - PDF / 1 -CSV)
  - Add user as Receiver (check box)

## Using the Query-Report Builder

If the predefined reports do not meet your needs, create a query from scratch, or clone and modify an existing query.

Before you start writing a query, plan carefully what you want the report to describe. There are two general use cases:

- You want to identify a specific occurrence in your system. This type of query has two parts. An event, or events, occurred in your system: this is defined by the conditions. What do you want to know about the system when this event occurred? These are the details (columns) presented in the report.
- You want status on some part of your system. In this case, you probably only need to specify the columns you want in the report.

First find the domain that covers the data you want. A domain contains a set of data related to a specific function or purpose, for example: data access, exceptions, policy violations. Each query is based on, and returns data from, one domain. For a description of all domains, see [Entities and Attributes in the domains](#). Each domain has one or more entities, which are groupings of attributes. Attributes are the fields that can be used as columns in the report. Some entities are included in more than one domain, to give you access to the relevant data. For example, the Session Entity is in both the Access domain and the Exceptions domain.

Data is tracking who did what, and when. Some details are static, some are dynamic. The entities, within the domain from top to bottom in the UI, start with static details, followed by non-static details. For example, in the Access domain, the first entity is client/server. Each client/server pair is saved once. The next entity is Session. The client/server pair has multiple sessions with non-static details, for example, session start and inactive flag. This creates a one-to-many relationship between the client/server and the sessions. To see each value of session start, you would need multiple rows. Instead of making your report unnecessarily long with each session start, you can use the count option to show the number of occurrences of session starts, and then drill down to see a more detailed report. The rule of thumb is: the higher up your main entity is in the GUI, the fewer rows and values you'll have in your report. The report is more manageable, and you can always drill down to see more details. For more information on how domains function in a query, and optimizing queries, see [Optimizing queries](#).

If you need details from two entities that are not included in one domain, you can create a custom domain (see [Custom Domains](#)).

A query returns data from one domain only. When the query is defined, one entity within that domain is designated as the main entity of the query. Each row of data returned by a query contains a count of occurrences of the main entity matching the values returned for the selected attributes, for the requested time period. This allows for the creation of two-dimensional reports from entities that do not have a one-to-one relationship.

Once you identify the domain, check the predefined reports in that domain to see if there is one close to what you want. If yes, you can clone and modify it. If not, create the query from scratch.

Define the report data (columns). You can choose columns from all the entities in the domain.

Optionally, define the conditions. Conditions, if you use them, are triggers for including the specific data in the report. A query on status, for example, does not need a trigger; you simply want to know the status of an element in your system. On the other hand, if you want to identify specific actions by a specific user on a group of databases, these are the query conditions. The conditions use the attributes in the domain, with operators. There is no intrinsic relationship between the conditions and the report columns. You can choose to add the attributes in the conditions as columns, or not.

You can also optionally defined build expressions or Having clauses on SQL statements.

Reports are the presentation of that data, created when you save your query, with the same name as the query. Default reports are tabular reports that reflects the structure of the query, with each attribute displayed in a separate column. All runtime parameters and presentation components of a tabular report can be customized.

The query builder has six rows for configuring the various aspects of the query, explained in the following sections.

There are buttons at the bottom of the Query-Report Builder page:

- Add to Dashboard: click to add the displayed report to a defined dashboard
- Add to My Custom Reports: Click to add to Reports > My Custom Reports
- Query Summary: Click to open a textual summary of the query

**A Caution about Full SQL Attributes in Queries** Beware of using the Full SQL attribute in a query. It may produce excessively large reports, because each distinct value of the attribute (the complete SQL query string in this case) will be returned in a separate row. On the other hand, the report may contain no information at all, or many blank columns where you are expecting Full SQL strings. Guardium captures Full SQL only when directed to do so by policy rules - and the rules may not have been triggered during the reporting period. Do not confuse the Full SQL attribute with the ability to drill down to the SQL for most queries in the Data Access domain having anything to do with SQL requests.

- [\*\*Optimizing queries\*\*](#)

To understand how to optimize queries, it is imperative to have an understanding of how queries work and how reported data is stored internally on the appliance. Each domain is associated with a particular predefined set of data. For example, Access domain for captured traffic, Exception domain for captured errors from the database server, or Guardium activity domain to monitor activities that are performed by Guardium users.

- [\*\*Creating a new query, modifying an existing query\*\*](#)

Search through all existing queries, or by domain, to copy and modify an existing query, or create a query from scratch.

- [\*\*Defining the query name and attributes\*\*](#)

Select the domain, then set the query name, the main entity, and configure roles, datamart, drilldown control, and API assignments.

- [\*\*Selecting the column display\*\*](#)

Choose the columns for your report from the attributes in all of the entities in the domain, and define the sort hierarchy.

- [\*\*Setting the sort order\*\*](#)

- [\*\*Defining the Query Conditions\*\*](#)

- [\*\*Adding a build expression on query condition\*\*](#)

Use this feature when you need to add a condition (including a user-defined string or a mathematical expression) that is based not on the entire content of the attribute as is, but on part of the attribute, a function of the attribute, or a function that combines more than one attribute.

- [\*\*Having conditions\*\*](#)

This row is available if "Group by" is required; when one or more columns use one of the following functions: count, min, max, average, sum.

- [\*\*Modifying the report display\*\*](#)

You can select the report type (tabular or chart), change the column names, and configure the color indication rules.

## Related concepts

---

- [Domains, Entities, and Attributes](#)

## Optimizing queries

---

To understand how to optimize queries, it is imperative to have an understanding of how queries work and how reported data is stored internally on the appliance. Each domain is associated with a particular predefined set of data. For example, Access domain for captured traffic, Exception domain for captured errors from the database server, or Guardium activity domain to monitor activities that are performed by Guardium users.

Most of the domains deal with small amounts of data and are irrelevant for this performance description. The Access domain is one domain that deals with large amounts of data that is used often. This domain contains database activity data that is captured by an appliance. This domain is composed of many tables with many millions of rows of data in each table. Carefully consider your decisions when you are designing queries in this domain. Each entity in the domain corresponds to an underlying table and has a list of attributes. Attributes correspond to fields in the table. When you select fields (attributes) from the Session entity and some other fields from the SQL entity, these two entities are joined to retrieve the data that you request. The more entities that are joined in your query, the more complex the final query is and the longer it takes to produce the results.

Guardium monitors and captures numerous details about database user activity. All of this information can be put into the following major categories.

- Who: Describes a connection to a database, who made a connection, and when the connection was made.
- What: Contains the SQL statements that ran on the database.

Connection details include attributes (fields), such as Server IP, DB Type, DB User Name. This information is recorded in the Client/Server and Session entities. Two entities are used: even though the login information (for example, IP, user name) of a user stays the same for every connection, every connection has unique information, for example, login time or client port. The relatively static, repeatable login information is stored in the Client/Server entity and the unique, connection-specific information is stored in the Session entity. Splitting information between two entities helps to reduce data redundancy and saves disk space.

In addition to login information, Guardium captures the SQL statements that are issued by the user or an application. The SQL statements are recorded in the SQL entity. To create queries with conditions on specific groups of tables, or sets of commands, Guardium parses captured SQLs to commands, objects, and fields, and places this information in three other entities: Commands, Objects, and Fields.

If you want to create a query that shows only the activity on a particular table, you can create a query with a condition, such as

```
WHERE OBJECT.OBJECT_NAME =
```

```
'myTable'
```

Or, if you want to create a query that shows only DML activity, you can create query condition, such as

```
WHERE COMMAND.VERB in group 'DML'
```

```
commands'
```

The redundancy here helps to create more efficient queries. When you create a query, you first enter a query name, then you select a main entity. It is important to select a main entity that indicates to the Query-Report builder the focal point for the new query and how to construct a query. Ultimately, it might also affect query performance.

For example, you can create two queries with identical fields, one with the main entity as Session, and the other with Command. The attributes are:

- Session start time
- Session end time
- Client IP
- Server IP
- DB user name
- Source program

The following query is generated by the Query-Report builder with the Session main entity:

```
select ... from GDM_ACCESS, GDM_SESSION where.... The following query is generated by the Query-Report builder with the Command main entity:
select
... from GDM_ACCESS, GDM_SESSION, GDM_CONSTRUCT_INSTANCE, GDM_SENTENCE where...
```

Both queries have the same columns. However, the first query joins two tables to produce the results and the second query has four tables that participated. The second query takes longer to complete. Even more important, most likely the second report has more records and some of the rows appear multiple times.

When Command is selected as the main entity, the Query-Report builder defines the report with the focus on "command". A session usually has many commands. Each command appears on the report in a separate row. Even if a session has no commands, there is a row for the session in the report, with an empty Command column. Main entities are organized hierarchically from high-level details to more granular. The main entity defines the level of details in the report. Selecting a main entity on too high a level in the list might limit your ability to select fields to report. An example is a single SQL statement with multiple fields. If you select SQL as a main entity, your level of detail is an SQL statement and each line in the report is dedicated to one SQL statement. This means that you cannot display fields in the same line because there is no space for multiple fields.

However, you can use the Count function to display total count of the fields in an SQL statement or the Max function to display the highest field value. If you query definition has SQL as the main entity for database activity, you cannot add the SQL Verb field from the Command entity because the Command entity is positioned lower than SQL entity in the entity list. Therefore, you cannot use the field value directly but you can apply the value to one of the math functions, such as Count, Min, or Max.

When you are designing a new query, consider the relationships between entities to avoid data redundancy in reports.

Certain database operations (such as GROUP BY, DISTINCT, ORDER BY, or HAVING clauses) provide flexibility to the Query-Report builder. However, these operations might take more processor time. If you have report performance issues, consider revising your report to limit the usage of these database operations.

In general, the data volume that is stored on the appliance is the major factor that can affect the report performance. When you tune the report performance, consider the following points:

- Define the purge process to run nightly.
- Configure the data retention period to the minimum that is allowed by your business requirements.
- Record Full SQL only when it is necessary (for example, to monitor sensitive objects or privileged users). Full SQL tables can add data volume quickly.
- Reduce the period of the report to have a positive effect on the report run time.

In centrally managed environments, reports frequently run on the aggregators instead of the collectors. Data that is exported from the collectors nightly in one-day chunks is transferred to the aggregator. On an aggregator, data from multiple collectors and multiple days is merged for reports. For efficiency reasons, not all of the data that is presented on an aggregator is merged and made available for reports. The merge period defines the date range that you can use in reports. It shows on top of every report you run. The default merge period is 14 days for interactive reports. The merge period is a derived internally. The merge period doesn't impact the date range available for audit processes.

Tip: Keep your purge period at a maximum of 90 days, and the maximum number of collectors that report to an aggregator at 10 to ensure timely data aggregation (and keep the merge period at 14).

## Creating a new query, modifying an existing query

Search through all existing queries, or by domain, to copy and modify an existing query, or create a query from scratch.

### About this task

Each domain contains a set of data related to a specific purpose or function (data access, exceptions, policy violations, and so forth). The names are self-explanatory, so you can easily select the relevant domain. For a description of all domains, see [Entities and Attributes in the domains](#).

### Procedure

1. Open the Query Builder by navigating to Investigate > Exceptions > Query-Report Builder, or Reports > Report Configuration Tools > Query-Report Builder.  
The list under Queries-Reports contains all queries in all the domains. Use the search to find a query.
2. Create a query using these guidelines:
  - Select an pre-defined query. A dialog box opens and you can choose to:
    - Open the original query (click Open original) to modify some attributes (for example: [Managing query security roles](#), [Adding a query to a datamart](#), [Modifying the query drilldown control](#), [Modifying the API assignment](#), [Creating dashboards and adding reports](#)). You cannot modify its query attributes or conditions.
    - Make a copy by clicking Make copy and giving it a new name. Continue with [Defining the query name and attributes](#).
  - Select the domain you want to query from the Select Domain drop-down. Select one for copying or click New . The New Query page opens. Continue with [Defining the query name and attributes](#).

- Select a user-defined query. Its properties open in the right hand pane. You can edit the query, or click  to copy the query. Continue with any query configuration tasks.
- Create a new query: Click New . The New Query page opens. Continue with [Defining the query name and attributes](#).

## Defining the query name and attributes

Select the domain, then set the query name, the main entity, and configure roles, datamart, drilldown control, and API assignments.

### About this task

When creating a query from scratch, the next step is to select the main entity (from the domain). The main entity that you select determines:

- The level of detail for the report. There is one row of data for each occurrence of the main entity included in the report. The location of the main entity within the hierarchy of entities is important in terms of what values can be displayed. Attributes in an entity at a higher level in the hierarchy can have a field mode of type value. Attributes in an entity at a lower level in the hierarchy cannot have a field mode of type value. You can see the hierarchy in the entities list in the query-report builder. The hierarchy is exactly as the list displays, from top to bottom.
- The time fields against which the Period From and Period To runtime parameters are compared to select the data in the report. The Query-Report Builder uses the main entity (among other parameters) to determine which time fields are used when defining the Period From and Period To values. This can be important for long-running sessions, such as when pooled sessions are kept open by an application server. When applicable, the Period Start/Period End from the Access Period entity is used, in other cases it chooses period values according to the main entity:
  - Session - the time stamp used is for the last update that is made to the session entity
  - Session Start - the starting time of the session entity is used
  - Session End - the ending time of the session entity is used
  - Full SQL - time stamp from Full SQL domain; query includes rows from the Full SQL domain even if not linked to values (for example - when Log Full Details is set, there are no values)
  - Full SQL Values - time stamp from the Full SQL domain; query includes rows only if they have values from the Full SQL domain even if not linked to the Field domain
  - Field SQL Values - time stamp from the Full SQL domain; query includes rows only if they have values from the Full SQL domain and they are linked to the Field domain

Other options in this row are:

- Partition optimization is enabled by default and improves query performance with partitioned database tables. You can disable this feature by clearing the Partition optimization check box. Partition optimization should not be disabled without the direction of Guardium support.
  - Run in Two Stages. Use this selection for two-stage execution for Audit tasks of type report. This applies to reports on queries on specific tables only. This two-stage mechanism applies to running queries as audit processes with columns and conditions only on the following entities: Access (client/server), Session, Access Period, Construct (SQL), Object, and Sentence (Command). This two-stage mechanism is not used if the query contains a condition with the **Like Group** operator or any alias-related operator (such as **In Aliases Group**) or the condition uses Having. By default, queries run in one stage. To disable two stage queries system wide, create the file: /var/log/guard/DontRunInTwoStages. Existence of this file indicates that the two stage method is NOT used.
- Note: Fields containing tuples (combined fields) in the Two Stages execution is not supported.

Note: The Main Entity drop-down list includes only primary entities. However, access to secondary entities (for example Session Start and Session End) can be done through its corresponding primary entity (for example, Session for Session Start and Session End).

### Procedure

1. For both cloned and new reports, in the right pane, enter a unique query name in the query name textbox. (You can use Ctrl+V to paste, or type the query name; right-click to copy the query name is not supported.)
2. Select the main entity from the drop-down list.
3. Click Next to select columns and save the query. Once the query is saved, additional buttons in this row become available, as relevant.
  - [Managing query security roles](#)  
By default, only the user that defines a query has access to the query. You can add and remove other roles (or all roles) to provide access to a query.
  - [Adding a query to a datamart](#)
  - [Modifying the query drilldown control](#)  
By default, the drill-down menu for a report includes all reports with run-time parameters that can be supplied by attributes from the report, which is given the usual security role restrictions.
  - [Modifying the API assignment](#)  
By default, the Guardium application comes with setup data that links many of the API functions to reports; providing users, through the GUI, with prepared calls to APIs from reporting data. Use API Assignment to link additional API functions to predefined Guardium reports or custom reports.

## Managing query security roles

By default, only the user that defines a query has access to the query. You can add and remove other roles (or all roles) to provide access to a query.

### About this task

The user that defines a query can grant access to additional users. Queries are completely filtered from the UI for users that do not have access to the query.

### Procedure

1. In the Query Name row, click Roles.  
The Assign Security Roles dialog opens.
2. Select or clear individual roles, or select All Roles to grant access to all roles.
3. Click OK.  
The roles are updated and the panel closes.

## Adding a query to a datamart

### About this task

If there is a predefined datamart based on the query, the predefined datamart output structure may not exactly match the query definition. For example, the predefined datamart **Export:Full SQL** does not have the field Original Timezone, but the predefined query **Export:Full SQL** does have the field. If you create a new datamart based on the query, it matches the query structure.

### Procedure

1. In the Query Name row, click Datamart.  
The Datamart Configuration dialog opens.
2. Select an existing datamart, or click New to create a new datamart.
3. Configure the extraction and click Apply.

## Modifying the query drilldown control

By default, the drill-down menu for a report includes all reports with run-time parameters that can be supplied by attributes from the report, which is given the usual security role restrictions.

### About this task

Drilldown control is accessed under Advanced Options in the Query Name row.

### Procedure

1. In the Query Name row, under Advanced options, click Drilldown Control to open the report's Drilldown Control panel.
2. Mark the checkbox for any report to be disabled, or clear the checkbox for any report to be enabled.
3. Click Apply. The system displays a message saying your changes were applied successfully.
4. Click Done when you are finished.

## Modifying the API assignment

By default, the Guardium application comes with setup data that links many of the API functions to reports; providing users, through the GUI, with prepared calls to APIs from reporting data. Use API Assignment to link additional API functions to predefined Guardium reports or custom reports.

### About this task

For more information on using linked API functions, see the documentation on GuardAPI Input Generation.

### Procedure

1. In the Query Name row, click show advanced options, then click API Assignment to open the API Assignment panel; showing the current API functions that are mapped to the selected report. If there are no fields in the report that are linked to API parameters, it might be irrelevant to link an API function to a report. The mapping of API parameters to report fields can be accomplished through both the GUI and the CLI. For additional information on mapping API parameters to report fields, see Mapping GuardAPI Parameters to Domain Entities and Attributes in the GuardAPI Input Generation section.
2. Click an API function to display a pop-up window of the current API - Report Parameter Mapping; showing the API parameters, if the API parameters are required, any default values, and if any of the report fields are currently mapped to those parameters.
3. Click the greater-than sign '>' to add the selected API function to the current list of functions that are assigned to this report.
4. Click Apply to save the changes.

## Selecting the column display

Choose the columns for your report from the attributes in all of the entities in the domain, and define the sort hierarchy.

### About this task

The number of columns cannot exceed:

- 30 string columns
- 25 numeric columns
- 6 text columns
- 8 date columns

## Procedure

---

1. In the Columns to Display area, select the columns you want to appear in the report. The drop-down list contains all the entities in the domain.
  2. Click an entity to open a list of its attributes, select all the attributes you want from all of the entities, and click Add.
  3. Optionally select Distinct to display one-row-per-value in the report (there is one row in the report for each combination of the column values). This option yields condensed reports, but option can impact performance.
  4. Optionally select Count. The Count option adds a count column (#) to the report, with the number of occurrences of the set of values in any one row. This count can be used for sorting. When using Count, you can have up to 4 columns in the report, including count.
  5. Arrange the attributes in the order you want them to display in the report, using the up and down arrows. Top to bottom in the UI is left to right in the report.
  6. For each attribute, select what to print for the field: its Value, Count (number of distinct values), Min, Max, Average (AVG) or Sum.
- 

## Setting the sort order

### About this task

---

The Sort by Count option is enabled if you selected the Count checkbox in the Selected Columns row. It sorts the rows by frequency of occurrence.

## Procedure

---

1. Open the Sort Results row.
  2. To sort by count, select Sort results by count.
  3. To sort by column:
    - a. Select Sort results by column.
    - b. Click and select the column that is the primary sort criterion. The ascending/descending dropdown defaults to ascending. Modify as relevant.
    - c. Repeat for additional columns, adding rows by clicking Then by.
    - d. Remove a column by clicking in the row.
- 

## Defining the Query Conditions

### About this task

---

Query conditions have the format: <And/Or> <Field> <Operator> <Value/Parameter/Group> <Value>

where:

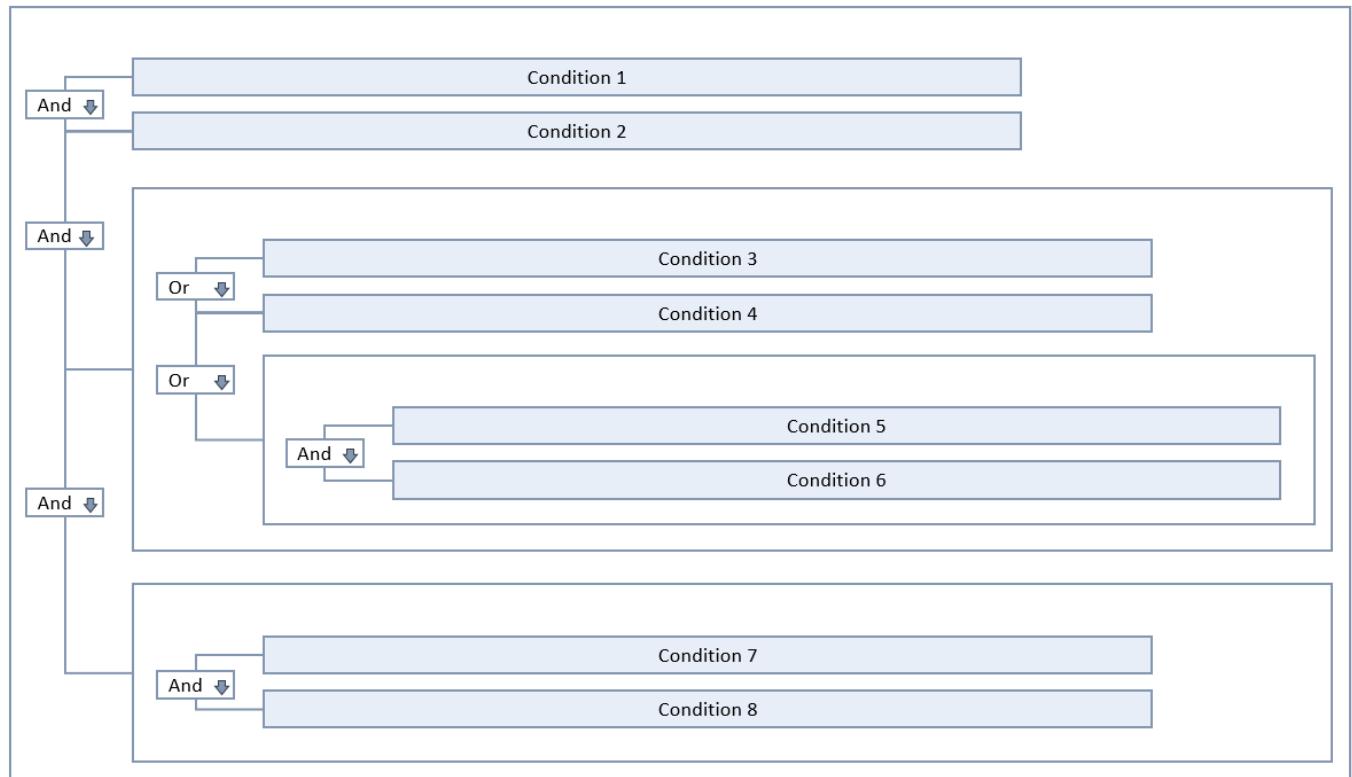
- And/Or: determines the relationship between the conditions or condition groups. The default is Add.
- Field: one of the fields in the query's domain
- Operator: the operator types depend on the selected field. For example, attributes that cannot be associated with groups do not have any of the group options (IN GROUP, LIKE GROUP).

| Operator                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <                        | Less than                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <=                       | Less than or equal to                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <>                       | Not equal to                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| =                        | Equal to                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| >                        | Greater than                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| >=                       | Greater than or equal to                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| CATEGORIZED AS           | Member of a group belonging to the category selected from the drop-down list, which appears when a group operator is selected.                                                                                                                                                                                                                                                                                                                                                                                    |
| CLASSIFIED AS            | Member of a group belonging to the classification selected from the drop-down list, which appears when a group operator is selected.                                                                                                                                                                                                                                                                                                                                                                              |
| IN ALIASES GROUP         | The operator works on a group of the same type as IN GROUP, however assumes the members of that group are aliases. Note that the IN GROUP/IN ALIASES GROUP operators expect the group to contain actual values or aliases respectively. An alias provides a synonym that substitutes for a stored value of a specific attribute type. It is commonly used to display a meaningful or user-friendly name for a data value. For example, Financial Server might be defined as an alias for IP address 192.168.2.18. |
| IN DYNAMIC ALIASES GROUP | The operator works on a group of the same type as IN DYNAMIC GROUP, however assumes the members of that group are aliases.                                                                                                                                                                                                                                                                                                                                                                                        |
| IN DYNAMIC GROUP         | Member of a group that is selected from the drop-down list in the runtime parameter column, which appears when a group operator is selected.                                                                                                                                                                                                                                                                                                                                                                      |
| IN GROUP                 | Member of the group that is selected from the drop-down list in the runtime parameter column, which appears when a group operator is selected. IN GROUP or IN ALIASES GROUP cannot both be used at the same time.                                                                                                                                                                                                                                                                                                 |
| IN PERIOD                | For a time stamp only, is within the selected time period                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| IS NOT NULL              | Attribute value exists, but might be blank or unprintable                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| IS NULL                  | Empty attribute                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| LIKE                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Operator                     | Description                                                                                                                                                                                                                                                                                                                                         |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LIKE GROUP                   | Matches a like value that is specified in the boxes. A like value uses the percent sign as a wildcard character, and matches all or part of the value. Alphabetic characters are not case-sensitive. For example, %tea% would match tea, TeA, tEam, steam. If no percent signs are included, the comparison operation is an equality operation (=). |
| NOT IN ALIASES GROUP         | The operator works on a group of the same type as NOT IN GROUP, however assumes the members of that group are aliases.                                                                                                                                                                                                                              |
| NOT IN DYNAMIC ALIASES GROUP | The operator works on a group of the same type as NOT IN DYNAMIC GROUP, however assumes the members of that group are aliases.                                                                                                                                                                                                                      |
| NOT IN DYNAMIC GROUP         | Not equal to any member of a group, which is selected from the drop-down list in the runtime parameter column, which appears when a group operator is selected.                                                                                                                                                                                     |
| NOT IN GROUP                 | Not equal to any member of the specified group, which is selected from the drop-down list in the runtime parameter column, which appears when a group operator is selected.                                                                                                                                                                         |
| NOT IN PERIOD                | For a time stamp only, not within the selected time period                                                                                                                                                                                                                                                                                          |
| NOT LIKE                     | Not like the specified value (see the description of LIKE)                                                                                                                                                                                                                                                                                          |
| NOT LIKE GROUP               | Not like the value that is specified in LIKE GROUP                                                                                                                                                                                                                                                                                                  |
| NOT REGEXP                   | Not matched by the specified regular expression                                                                                                                                                                                                                                                                                                     |
| REGEXP                       | Matched by the specified regular expression For detailed information about how to use regular expressions, see Regular Expressions.                                                                                                                                                                                                                 |

- Value/Parameter/Group: depends on the operator.
  - Value: A constant with which the field is compared.
  - Parameter: The name of a parameter that gets its value in run time. The parameter name cannot be any of: QUERY\_FROM\_DATE, QUERY\_TO\_DATE, REMOTE\_SOURCE, SHOW\_ALIASES, FETCHSIZE, REFRESHRATE, current\_title, action, user, group, role, js\_peid, eventsubmit\_doupdate, page, \_skin, template, media-type. The parameter name must start with a letter and can only contain letters, digits, and underscore.
  - Group: A drop-down list of the groups that match the type of the field. The groups with the same type as the field appear first, in alphabetic order. Then groups with all types appear, grouped by their type. The group types are ordered alphabetically and so are the groups under each type. Note that in some cases there may be several group types that match the field type. For example, there are several group types that match Client IP: Client IP/DB User, Client IP/Src App./DB User, Client IP/Src App./DB User/ServerIP/Svc. Name
- Value: depends on the Operator and the Value/Parameter/Group

Query conditions can include both individual conditions and groups of conditions. When adding a condition or a condition to a group, the default conjunction is Add. You can change this to Or. Each condition group is processed as though it is in parenthesis. The following figure presents a query with two conditions and two condition groups specifying: condition 1 **and** condition 2 **and** (condition 3 **or** condition 4 **or** (condition 5 **and** condition 6) **and** (condition 7 **and** condition 8)).



**Escaping backslash (\) characters:** To correctly escape a backslash character for use in a query condition, use four backslash characters. For example, to specify domain\user you would enter domain\\\\\\user.

## Procedure

1. In the Conditions row, click Edit. The Conditions area expands.
2. To add a condition, click Add Condition and select values in the drop-downs for the first query condition.
3. To add a condition group, click Add Condition Group and select values in the drop-downs for the conditions in the group.
4. Repeat as relevant.

5. Click Save.

## Adding a build expression on query condition

Use this feature when you need to add a condition (including a user-defined string or a mathematical expression) that is based not on the entire content of the attribute as is, but on part of the attribute, a function of the attribute, or a function that combines more than one attribute.

Once the query conditions are saved, there is an Add Expression icon  icon, next to the query conditions, that opens the Build Expression pane. Use it to add user-defined strings and mathematical expressions.

When there is a build expression defined, there is a red asterisk next to the Build Expression icon .

An example:

Return the location of the string **150 . 1**, from the value **192.150.1.x.**, where the string **150 . 1** is at the fifth character of the value. The string **150 . 1** represents all instances of Client IP matching the 5 characters listed.

When the function is run in the Expression field, it returns a value, and that value should be in the entry box.

Use the function, **INSTR(:attribute, '150 . 1')** with a "5" value in the entry box next to the Add Expression icon to return the records with **150 . 1** in the fifth location.

If the function is **INSTR(:attribute, '150 . 1') = 5**, then it becomes a Boolean phrase, and the only values in the entry box are 0 or 1.

Type the **INSTR(:attribute, '150 . 1')** expression in the separate Build Expression window.

Test the validity of the expression in the Build Expression window.

Another example: **LENGTH(:attribute) >= 40**, which returns the length of any SQL statement greater than 40 characters. The expression might or might not contain references to the actual attribute and can also contain references to other attributes.

## Having conditions

This row is available if "Group by" is required; when one or more columns use one of the following functions: count, min, max, average, sum.

Having Conditions function like other query conditions, except that they have an additional aggregation function field. Their format is: <And/Or> <field> <aggregation function> <operator> <value/parameter/group> <value>. The aggregation function can have the values:

- Count
- Min
- Max
- Avg.
- Having

The operators available in the Having clause are:

- Smaller than (<)
- Smaller than or equal to (<=)
- Not equal to (<>)
- Equal to (=)
- Greater than (>)
- Greater than or equal to (>=)

## Modifying the report display

You can select the report type (tabular or chart), change the column names, and configure the color indication rules.

### About this task

The Chart type report is available only if one of these is true:

- The Count checkbox is selected on the query level.
- All the columns in the query are numeric.

### Procedure

1. Select the report type. By default it is Tabular. If you select Chart, choose a chart type from the type drop-down list.
2. In the Column Heading section, you can change the names of the columns from the attribute name to a name of your choice.
3. In the Color Indication Rules section:

- a. Create a rule by clicking , and assign a color to the rule. The first match (from top to bottom) determines the color in the report.
- b. Add more rules by clicking , and assign a color to the rule.
- c. Modify the rule order using  and .

# Domains, Entities, and Attributes

Each domain contains a set of data stored in Guardium that relates to a specific purpose or function (data access, exceptions, policy violations, and so forth). The data is grouped by entities. An entity is a set of related attributes, and an attribute is basically a field value.

Access to the domains is controlled by security roles. Each Guardium role typically has access to a subset of domains, depending on the function of that role within the company. Guardium admin role users typically have access to all reporting domains.

Some domains are available only when optional components (CAS, or Classification, for example) are installed. Other domains are available by default to Guardium admin role users only, for example report information pertaining to the Guardium appliance such as archiving activity.

Similarly, not all attributes are available for all database protocols. When using the query builder, if you notice that an entity or attribute described in the documentation does not appear in the UI, that entity or attribute is not available for the selected database type.

- [\*\*Entities and Attributes in the domains\*\*](#)

This topic contains a description of the entities and attributes in each domain.

## Entities and Attributes in the domains

This topic contains a description of the entities and attributes in each domain.

For z/OS data sources (Db2, Data Sets, and IMS), there are data-source-specific attributes and the meaning of existing attributes may differ than what is described here. For more information on entities and attributes specific to z/OS data sources, see the following:

- [\*\*Report entities and attributes for Data Sets\*\*](#)
- [\*\*Report entities and attributes for DB2 for z/OS\*\*](#)
- [\*\*Report entities and attributes for IMS\*\*](#)

- [\*\*Access domain\*\*](#)

This domain contains traffic data collected by the inspection engines and other sources such as universal connectors and streaming data sources, every time a request is sent to a server being monitored. It includes all of the client/server, session, SQL, and access periods related data. This topic describes the domain's entities and attributes.

- [\*\*Access Policy domain\*\*](#)

Use the Access Policy domain to track all available policies on system. This topic describes the domain's entities and attributes.

- [\*\*Aggregation/Archive domain\*\*](#)

Aggregation and archiving activity: archive, send, purge, and so on. This topic describes the domain's entities and attributes.

- [\*\*Alert domain\*\*](#)

This domain contains data on alerts generated and sent by Guardium. This topic describes the domain's entities and attributes.

- [\*\*Analytic Threat Analytics domain\*\*](#)

This domain has detailed descriptions of active threat analytics. This topic describes the domain's entities and attributes.

- [\*\*Analytic Outlier Details domain\*\*](#)

This domain has detailed descriptions of activities and errors that have been identified as outliers. This topic describes the domain's entities and attributes.

- [\*\*Analytic Outliers Status domain\*\*](#)

This domain describes the outlier mining process and its results. This topic describes the domain's entities and attributes.

- [\*\*Analytic Outlier Summary domain\*\*](#)

A summary of the outliers that occurred during the last hour on a source. This topic describes the domain's entities and attributes.

- [\*\*Application Data domain\*\*](#)

Connection, session, and application data recorded for special non-Guardium application (Siebel and SAP, for example). This topic describes the domain's entities and attributes.

- [\*\*Audit Process domain\*\*](#)

The execution of audit processes and the distribution of results. : entities and attributes

- [\*\*Auto-discovery domain\*\*](#)

Database auto-discovery activity, including all processes that have been run, and the hosts and ports discovered. This topic describes the domain's entities and attributes.

- [\*\*BigData Intelligence Buff Usage Monitor domain\*\*](#)

Shows the aggregate of all Sniffer Buffer Usage Entities. This topic describes the domain's entities and attributes.

- [\*\*BigData Intelligence Classification Process Log domain\*\*](#)

Reports on classifier process logs. This topic describes the domain's entities and attributes.

- [\*\*BigData Intelligence Classifier Results domain\*\*](#)

Reports on classifier process results. This topic describes the domain's entities and attributes.

- [\*\*BigData Intelligence Databases Discovered domain\*\*](#)

Reports on discovered databases. This topic describes the domain's entities and attributes.

- [\*\*BigData Intelligence Discovered Instances domain\*\*](#)

Reports on instances that have been discovered by GIM. This topic describes the domain's entities and attributes.

- [\*\*BigData Intelligence Exception domain\*\*](#)

All of the exceptions and exception-related data. These are SQL exceptions sent from a database server and collected by inspection engines, as well as exceptions generated by Guardium itself. This topic describes the domain's entities and attributes.

- [\*\*BigData Intelligence Full SQL domain\*\*](#)

You can create full SQL entities by using only the following policy rule actions: Log Full Details, Log Full Details With Values, Log Full Details Per Session, or Log Full Details Per Session With Values.

- [\*\*BigData Intelligence Installed Patches domain\*\*](#)

Reports on installed patches. This topic describes the domain's entities and attributes.

- [\*\*BigData Intelligence Instance domain\*\*](#)  
This domain contains traffic data collected by the inspection engines every time a request is sent to a server being monitored. It includes all of the client/server, session, SQL, and access periods related data. This topic describes the domain's entities and attributes.
- [\*\*BigData Intelligence Outliers List Enhanced domain\*\*](#)  
Detailed description of activities and errors that have been identified as outliers. This topic describes the domain's entities and attributes.
- [\*\*BigData Intelligence Outliers Summary Enhanced domain\*\*](#)  
A summary of the outliers in one hour granularity. This topic describes the domain's entities and attributes.
- [\*\*BigData Intelligence Policy Violations domain\*\*](#)  
All policy violation data, for all violations of the policy detected by the Guardium inspection engines or STAPs. This topic describes the domain's entities and attributes. This topic describes the domain's entities and attributes.
- [\*\*BigData Intelligence Session domain\*\*](#)  
Reports on Client/Server database session. This topic describes the domain's entities and attributes.
- [\*\*BigData Intelligence STAP Status domain\*\*](#)  
Reports on status of S-TAPs. This topic describes the domain's entities and attributes.
- [\*\*BigData Intelligence System Info domain\*\*](#)
- [\*\*BigData Intelligence VA Results domain\*\*](#)
- [\*\*CAS Changes domain\*\*](#)  
Tracks changes to monitored items (files, registry variables, etc.). This topic describes the domain's entities and attributes.
- [\*\*CAS Config domain\*\*](#)  
Tracks CAS host configurations, where a configuration is the application of one or more template sets to a specific database server host. From configuration instances you can see which items within template sets are enabled or disabled, or exactly which files are selected and monitored (or not) by file name pattern templates. This topic describes the domain's entities and attributes.
- [\*\*CAS Host History domain\*\*](#)  
Tracks CAS host events, including servers or clients going in or out of service. This topic describes the domain's entities and attributes.
- [\*\*CAS Templates domain\*\*](#)  
Track CAS template definitions. Templates identify items to be monitored for changes. Monitored items can be files, environment or registry variables, OS or SQL script output sets, or the set of logged on users. This topic describes the domain's entities and attributes.
- [\*\*Catalog domain: entities and attributes\*\*](#)  
The Guardium catalog tracks where every archive or backup is sent. The catalog domain presents catalog details.
- [\*\*Classification Process Results domain\*\*](#)  
Reports on classifier process runs and results. This topic describes the domain's entities and attributes.
- [\*\*CM Buffer Usage Monitor domain\*\*](#)  
Shows the aggregate of all Sniffer Buffer Usage Entities that have been uploaded to the central manager. This topic describes the domain's entities and attributes.
- [\*\*Comments domain\*\*](#)  
User defined comments for various Guardium components. This topic describes the domain's entities and attributes.
- [\*\*Custom DB Usage domain\*\*](#)  
Custom DB statistics. This topic describes the domain's entities and attributes.
- [\*\*DB Default Users Enabled domain\*\*](#)  
Details on whether default users are enabled. This topic describes the domain's entities and attributes.
- [\*\*Discovered Instances domain\*\*](#)  
Instances that have been discovered by GIM. This topic describes the domain's entities and attributes.
- [\*\*Distributed Datamart domain\*\*](#)  
Data on distributed data marts. This topic describes the domain's entities and attributes.
- [\*\*Eagle Eye domain\*\*](#)  
Data on the Threat Detection Analytics. This topic describes the domain's entities and attributes.
- [\*\*Exceptions domain\*\*](#)  
This domain contains traffic details: all of the exceptions and exception-related data. These are SQL exceptions sent from a database server and collected by inspection engines, as well as exceptions generated by Guardium itself. This topic describes the domain's entities and attributes.
- [\*\*FAM domain\*\*](#)  
This domain describes file entitlement (privileges) reports. This topic describes the domain's entities and attributes.
- [\*\*FAM groups domain\*\*](#)  
FAM groups are used in cases where file privileges are given to user groups that are under users domain. This domain has entities for mapping from users to groups. Only local groups are supported. This topic describes the domain's entities and attributes.
- [\*\*FAM System domain\*\*](#)  
The FAM system domain describes FAM configurations. This topic describes the domain's entities and attributes.
- [\*\*File Activity Monitor domain\*\*](#)  
This domain contains file entitlement and classification entities. This topic describes the domain's entities and attributes.
- [\*\*Flat Log domain\*\*](#)  
Flat log processing activity. This topic describes the domain's entities and attributes.
- [\*\*GIM Clients domain\*\*](#)  
This topic describes the domain's entities and attributes.
- [\*\*GIM Events domain\*\*](#)
- [\*\*Group domain\*\*](#)  
Membership in Guardium groups. This topic describes the domain's entities and attributes.
- [\*\*Guard Process Log domain\*\*](#)  
Logs of processes running on Guardium. This topic describes the domain's entities and attributes.
- [\*\*Guardium Activity domain\*\*](#)  
All modifications performed by Guardium users to any Guardium entity, such as a report or query definition or modification. This topic describes the domain's entities and attributes.
- [\*\*Guardium Jobs Queue domain\*\*](#)  
This topic describes the domain's entities and attributes.
- [\*\*Guardium Login domain\*\*](#)  
All Guardium user login and logout information. This topic describes the domain's entities and attributes.
- [\*\*IMS Event domain\*\*](#)  
This topic describes the domain's entities and attributes.
- [\*\*Installed Patches domain\*\*](#)  
Reports on installed patches. This topic describes the domain's entities and attributes.
- [\*\*Installed Policy domain\*\*](#)  
Description of policy parameters and rules for the installed policy. The Installed Policy domain supports multiple policies and multiple actions per rule. This topic describes the domain's entities and attributes.

- **[Managed units domain](#)**  
The managed units domain describes the managed units and the managed unit groups in your environment. This topic describes the domain's entities and attributes. This domain cannot be used as custom domain
- **[Parser Errors domain](#)**  
This topic describes the domain's entities and attributes.
- **[Policy Violations domain](#)**  
All policy violation data, for all violations of the policy detected by the Guardium inspection engines or STAPs. This topic describes the domain's entities and attributes.
- **[Policy Violations Summary domain](#)**  
All policy violation data, for a summary of all violations of the policy detected by the Guardium inspection engines or STAPs. This topic describes the domain's entities and attributes.
- **[Query Rewrite domain](#)**  
This topic describes the domain's entities and attributes.
- **[Runtime Sensitive Object Identifier domain](#)**  
This topic describes the entities and attributes for the Runtime Sensitive Object Identifier domain.
- **[Security Assessment Result domain](#)**  
Records the results of vulnerability assessment processes. This topic describes the domain's entities and attributes.
- **[Sniffer Buffer Usage Monitor domain](#)**  
Inspection engine statistics. This topic describes the domain's entities and attributes.
- **[S-TAP Status domain](#)**  
This topic describes the domain's entities and attributes.
- **[S-TAP status history domain](#)**  
This topic describes the domain's entities and attributes.
- **[S-TAP Statistics domain](#)**  
This topic describes the domain's entities and attributes.
- **[S-TAP verification domain](#)**  
This topic describes the domain's entities and attributes.
- **[Unit Utilization Levels domain](#)**  
This topic describes the domain's entities and attributes.
- **[User/Role/Application domain](#)**  
Relates Guardium users, roles and applications (to report on who has access to which Guardium applications). This topic describes the domain's entities and attributes.
- **[VA Summary domain](#)**  
This topic describes the domain's entities and attributes.
- **[VA Tests domain](#)**  
Reports on tests that are available for security assessments.
- **[Value Change domain](#)**  
All changes tracked by the trigger-based value change application. This topic describes the domain's entities and attributes.

## Access domain

This domain contains traffic data collected by the inspection engines and other sources such as universal connectors and streaming data sources, every time a request is sent to a server being monitored. It includes all of the client/server, session, SQL, and access periods related data. This topic describes the domain's entities and attributes.

Available to roles: all

## Client/Server Entity

This entity describes a specific client-server connection. An instance is created each time a unique set of attributes (excluding the Timestamp) is detected.

Note: For Access Tracking only, Client/Server Entity name appears in the menu as two possible entities - Client/Server and Client/Server By Session. Client/Server By Session gets its count from the Client/Server and date conditions from the Session.

Client/Server gets its count from the Client/Server and date conditions also from the Client/Server.

If you select Client/Server, then the query is populated with ATTRIBUTE\_ID = 1. If you select Client/Server By Session, then the query is populated with MAIN\_ATTRIBUTE\_ID = 0.

| Attribute                                    | Description                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access ID                                    | A unique identifier for this unique set of client/server connection attributes. Only available to users with the admin role.                                                                                                                                                                                                                                                    |
| Analyzed Client IP                           | Applies only to encrypted traffic; when set, client IP is set to zeroes.<br>Analyzed Client IP contains the IP for encrypted sessions. For unencrypted sessions Analyzed Client IP will be the same as Client IP.                                                                                                                                                               |
| Client Host Name                             | Client host name.                                                                                                                                                                                                                                                                                                                                                               |
| Client IP                                    | Client IP address. For ASO traffic, CLIENT_IP is not the actual client IP; use the Analyzed Client IP, which is the correct IP. For Oracle ASO encrypted IPv6 traffic (local as well as remote), use the Client Host Name to identify the actual client session, due to limitations. For SSL traffic, Client IP is not the actual client IP and there is no Analyzed Client IP. |
| ClientIP / DBUser                            | Paired attribute value consisting of the client IP address and database user name.                                                                                                                                                                                                                                                                                              |
| Client IP/Src App/DB User/Server IP/Svc Name | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                             |
| Client IP/Src App/User                       | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                             |
| Client MAC                                   | Client hardware address.                                                                                                                                                                                                                                                                                                                                                        |

| Attribute                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Client OS                  | <p>Client operating system.</p> <p>For Teradata, as there is no direct information about client/server OS, instead, the data format type is used; indicating how integer data are stored during db session. This has a close relation to the platform being used and may appear as follows:</p> <p>IBM MAINFRAME // IBM mainframe data format</p> <p>HONEYWELL MAINFRAME // Honeywell mainframe data format</p> <p>AT&amp;T 3B2 // AT&amp;T 3B2 data format.</p> <p>INTEL 8086 // Intel 8086 data format (IBM PC or compatible)</p> <p>VAX // VAX data format</p> <p>AMDAHL // Amdahl data format</p>                                                                                                                                         |
| DB Protocol                | Protocol specific to the database server For example, DRDA (Db2), TNS (Oracle), or TDS (MS SQL Server).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| DB Protocol Version        | Protocol version for the DB Protocol.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| DB User Name               | Database user name: user that connected to the database, either local or remote.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Last Used                  | The timestamp of the last time the data was used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Network Protocol           | Network protocol used (such as TCP or UDP. For K-TAP on Oracle, this displays as either IPC or BEQ)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| OS User                    | OS user as reported by the database client where supported by the database type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Server Description         | Server description (if any). For example, displays cluster name of the Cloudera Data Platform.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Server Host Name           | Server host name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Server IP                  | Server IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Server IP/DB user          | Paired attribute value consisting of Server IP address and database user name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Server IP/Svc Name/DB User | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Server OS                  | <p>Server operating system.</p> <p>For Informix, the OS may appear as follows:</p> <p>IEEEM indicating Unix or JDBCIEEEI indicating WindowsDEC indicating DEC Alpha</p> <p>For Teradata, as there is no direct information about client/server OS, instead, the data format type is used; indicating how integer data are stored during db session. This has a close relation to the platform being used and may appear as follows:</p> <p>IBM MAINFRAME // IBM mainframe data format</p> <p>HONEYWELL MAINFRAME // Honeywell mainframe data format</p> <p>AT&amp;T 3B2 // AT&amp;T 3B2 data format.</p> <p>INTEL 8086 // Intel 8086 data format (IBM PC or compatible)</p> <p>VAX // VAX data format</p> <p>AMDAHL // Amdahl data format</p> |
| Server Type                | The type of database monitored, such as Dd2, Oracle, or Teradata.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Service Name               | Service name for the interaction. In some cases (AIX shared memory connections, for example), the service name is an alias that is used until the actual service is connected. In those cases, once the actual service is connected, a new session is started - so what the user experiences as a single session is logged as two sessions.<br>For Teradata, Service name contains the session logical host id value.                                                                                                                                                                                                                                                                                                                         |
| Source Program             | Source program as reported by the database client where supported by the database type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Client/ Server by session  | Client/Server by session is also a Main Entity. Access this secondary entity by clicking on the Client/Server primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Timestamp                  | The time on the collector when the client <b>first</b> connected to the server. For example, if a client is connecting to the server in the same way many days in a row this timestamp will be the time of the first connection. This may even be before the purge days of the appliance.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Timestamp Date             | Date only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Timestamp Time             | Time only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Timestamp Weekday          | Weekday only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Timestamp Year             | Year only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## Session Entity

This entity is created for each Client/Server database session.

| Attribute       | Description                                                                                                                                                                                                                                    |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access ID       | A unique identifier for this unique set of client/server connection attributes. Only available to users with the admin role.                                                                                                                   |
| Client Port     | Client port number.                                                                                                                                                                                                                            |
| Database Name   | Name of database for the session.<br>For Oracle, Database Name may contain additional and application specific information such as the currently executing module for a session that has been set in the MODULE column of the V\$SESSION view. |
| Duration (secs) | Indicates the length of time between the Session Start and the Session End (in seconds).                                                                                                                                                       |
| Global ID       | Uniquely identifies the session - access. Only available to users with the admin role.                                                                                                                                                         |
| Ignored Since   | Timestamp created when starting to ignore this session.                                                                                                                                                                                        |

| Attribute             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Inactive Flag         | <ul style="list-style-type: none"> <li>-1: Session closed by timeout.</li> <li>0 (default): Open for sessions generated by SQL package.</li> <li>1: Closed (disconnect/ logout received).</li> <li>2: Closed due to timeout on Guardium system. The session is reopened when traffic is regenerated in the session.</li> <li>3: For sessions generated from non-SQL packets.</li> </ul>                                                                                                                                                                                                                  |
| Old Session ID        | Points to the session from which this session was created. Zero if this is the first session of the connection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Original Timezone     | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00, This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |
| Process ID            | The process ID of the client that initiated the connection (not always available).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Server Port           | Server port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Session Encrypted     | Whether the session is encrypted. 0: no; 1: yes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Session End           | The time on the DB server when the session ended. Session End is also a Main Entity. Access this secondary entity by clicking on the Session primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Session End Date      | Date only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session End Time      | Time only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session End Weekday   | Weekday only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Session End Year      | Year only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session ID            | Uniquely identifies the session. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Session Ignored       | A Yes indicates that the session was ignored using the IGNORE SESSION policy action.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Session Start         | The time on the DB server when the session started. Session Start is also a Main Entity. Access this secondary entity by clicking on the Session primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Session Start Date    | Date only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Session Start Time    | Time only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Session Start Weekday | Weekday only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Session Start Year    | Year only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Terminal Id           | Terminal ID of the connection, used internally to resolve session information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Timestamp             | The time on the collector when the session information was most recently updated. Initially, a timestamp created for the first request on a client-server connection where there is not an active session in progress. Later, it is updated when the session is closed, or when it is marked inactive following an extended period of time with no observed activity. When tracking Session information, you are probably more interested in the Session Start and Session End attributes than the Timestamp attribute. If the session is closed it is the same time as the Session End.                 |
| Timestamp Date        | Date only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timestamp Time        | Time only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timestamp Weekday     | Weekday only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Timestamp Year        | Year only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| TTL                   | Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Uid Chain             | For a session reported by Unix S-TAP (K-TAP mode only), or FAM on Windows, this shows the chain of OS users, when users <b>su</b> with a different user name. For more information, see <a href="#">Linux-Unix: UID chains</a> and <a href="#">UID chain for FAM</a> .                                                                                                                                                                                                                                                                                                                                   |
| Uid Chain Compressed  | The UID chain excluding the first user and the last user. For more information, see <a href="#">Linux-Unix: UID chains</a> and <a href="#">UID chain for FAM</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Client/Server Session Entity

| Attribute                                                     | Description                                                                                         |
|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Client IP/Src App/DB User/Server IP/Svc. Name/OS User/DB Name | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> . |
| Server IP/Server Port                                         | Server IP/Server Port                                                                               |

## PIM Session Entity

The Privileged Information Management (PIM) entity. For more information, see [PIM Integration with Guardium DAM](#).

| Attribute          | Description                 |
|--------------------|-----------------------------|
| Checkin Timestamp  | Time of credential checkin  |
| Checkout Timestamp | Time of credential checkout |
| Credential Tag     |                             |
| Global Id          |                             |
| Justification      |                             |

| Attribute    | Description                                           |
|--------------|-------------------------------------------------------|
| Resource Tag |                                                       |
| Session Id   |                                                       |
| User name    | The name of the user who checked out the credentials. |

## Access Period Entity

Access Periods are related to Sessions. By default, an access period is one hour long, but this can be changed by the Guardium administrator in the Inspection Engine Configuration (it corresponds to the Logging Granularity).

| Attribute              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application Event ID   | The application event ID if set from the API. Appears only when the main entity for the query permits this level of detail. Not available if either Client/Server or Session is the main entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Avg Execution Ack Time | Average Execution Acknowledged time in milliseconds                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Avg Records Affected   | The average number of records affected. Appears only when the main entity for the query permits this level of detail. Not available if either Client/Server or Session is the main entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Application User       | Can be one of the following attributes: <ul style="list-style-type: none"> <li>The Application User when identified by <a href="#">application user translation</a>.</li> <li>The Application Event Str when identified by the GuardAppUser API.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Average Execution Time | The average command execution time during the period. This is for SQL statements only. It does not apply to FTP traffic.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Construct ID           | Uniquely identifies a command construct (for example, select a from b). Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Egress Kbyte count     | Records the number of bytes in responses.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Failed Sqls            | The number of failed SQL requests. See note at the end of the table. Appears only when the main entity for the query permits this level of detail. Not available if either Client/Server or Session is the main entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Ingress Kbyte count    | Records the number of bytes in requests.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Instance ID            | Uniquely identifies an instance of a construct. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Original Timezone      | The UTC offset.<br>This is to point out that a UTC offset should be set so that the time from two different collectors that are in two different time zones aggregate correctly. If the offset was not set then there would exist a condition where users would not really be able to determine or see a true representation of when things happened in relation to time.<br><br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00. This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |
| Period End             | The time on the collector when the period, as defined by the logging granularity on the appliance (default 1 hour), ended.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Period End Date        | Date only from the period end attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Period End Time        | Time only from the period end attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Period End Weekday     | Weekday only from the period end attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Period Start           | The time on the collector when the period, as defined by the logging granularity on the appliance (default 1 hour), started.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Period Start Date      | Date only from the period start attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Period Start Time      | Time only from the period start attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Period Start Weekday   | Weekday only from the period start attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Response Length        | The length of the sniffer response for a SQL instance. Not supported for Db2 z/OS systems. For more information, see <a href="#">store log_general_response_length</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Session ID             | Uniquely identifies a session. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Show Seconds           | If a the number of accesses per second is being tracked, this contains counts for each second in the access period (usually one hour).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Successful Sqls        | The number of successful SQL requests. See note at the end of the table. Appears only when the main entity for the query permits this level of detail. Not available if either Client/Server or Session is the main entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Timestamp              | The time on the collector when an SQL construct was executed most recently <i>within a session and within a time period</i> . If the same SQL construct is run 10 times within the same session and time period, it shows the time of the most recent run for all 10 SQLs. This timestamp is the most appropriate to use along with the SQL attribute in reports.<br><br>Note: Universal Connector traffic may be delayed. In those cases the Timestamp is the time of on the Collector for the most recent update to the SQL construct record for the session within a time period. Period start still reflects the time of SQL execution according to the audit data source, not the time of record update.                               |
| Total Access           | Total count of construct instances for this access period. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Total Records Affected | The total number of records affected. Appears only when the main entity for the query permits this level of detail. Not available if either Client/Server or Session is the main entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Attribute                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Total Records Affected (Desc) | <p>If the Total Records Affected attribute is a character string instead of a number, that value appears here (for example, Large Results Set, or N/A). Appears only when the main entity for the query permits this level of detail. Not available if either Client/Server or Session is the main entity.</p> <p>Records affected - Result set of the number of records which are affected by each execution of SQL statements.</p> <p>Note: The records affected option is a sniffer operation which requires sniffer to process additional response packets and postpone logging of impacted data which increases the buffer size and might potentially have a adverse effect on overall sniffer performance. Significant impact comes from really large responses. To prevent large amount of overhead associated with this operation, Guardium uses a set of default thresholds that allows sniffer to decide to skip processing operation when exceeded.</p> <p>You can use the <b>store max_results_set_size</b>, <b>store max_result_set_packet_size</b>, and <b>store max_tds_response_packets</b> CLI commands to set levels of granularity.</p> <p>Example of result set values:</p> <ul style="list-style-type: none"> <li>Case 1, record affected value, positive number. This represents correct size of the result set.</li> <li>Case 2, record affected value, -2. This means number of records exceeded configurable limit (This can be tuned through CLI commands).</li> <li>Case 3, record affected value, -1. This shows any unsupported cases of packets configurations by Guardium.</li> <li>Case 4, record affected value, -2. If the result set is sent by streaming mode.</li> <li>Case 5, record affected value, less than -2. Intermediate result during record count to update user about current value, ends up with positive number of total records. For example, the server returns 1000 records in 4 packets: <ul style="list-style-type: none"> <li>Packet #1 250</li> <li>Packet #2 200</li> <li>Packet #3 250</li> <li>Packet #4 200</li> </ul> </li> </ul> <p>Then records affected are reported as</p> <ul style="list-style-type: none"> <li>Packet #1 -250</li> <li>Packet #2 -500</li> <li>Packet #3 -750</li> <li>Packet #4 1000</li> </ul> |

## Changed Data Value Entity

This entity is used with the IBM InfoSphere Change Data Capture (InfoSphere CDC) replication solution that allows the replication to and from supported databases. Maintenance of replicated databases can be used to reduce processing overheads and network traffic.

IBM® Guardium® Customers with Database Activities Monitoring will have access to InfoSphere CDC.

This Guardium feature uses Java CDC user exit to send value change information to the Guardium collector.

User exits for InfoSphere CDC lets the user define a set of actions the InfoSphere CDC can run before or after a database event occurs on a specified table.

| Attribute   | Description                         |
|-------------|-------------------------------------|
| Full SQL ID | Unique identifier for the Full SQL. |
| Table Name  | Table Name from database            |
| Column Name | Column Name from database           |
| Old Value   | Value before the change.            |
| New Value   | Value after the change.             |
| Timestamp   | Time the record was created.        |

Two files that need to be installed on the Database Server are for the Guardium agent that interfaces with IBM's InfoSphere Change Data Capture (InfoSphere CDC) application. They are in the sources/apps/GuardCDC/lib/ directory of the build. These files are: protobuf-java-2.4.1.jar; and, GuardCdc.jar

### Instructions for installation

Prerequisites - the InfoSphere Change Data Capture (InfoSphere CDC) application must already be installed on the DB Server.

Steps to install the Guardium agent on the Database server:

1. Copy these two files to the RepEngine/lib/ directory of the cdchome directory. An example of the full path would be /cdchome/cdc6.5.2/RepEngine/lib/
2. Unzip each file
3. Edit the guard\_cdc\_user\_exit\_config.xml file to add the Guardium\_Host name. An example of where this file would be located is /cdchome/cdc6.5.2/RepEngine/lib/com/guardium/cdc/userexit/
4. Configure InfoSphere CDC to write to the GuardiumAgent. There are multiple steps to set up and configure the CDC application. These steps can be obtained from the InfoSphere CDC development/support team at IBM.

## App User Name Entity

This entity displays the username from the App Event if the App Event exists. Otherwise, the user name displays from the Construct Instance.

| Attribute     | Description                                      |
|---------------|--------------------------------------------------|
| APP User Name | Unique identifier for this App User Name entity. |

## FULL SQL Values Entity

These entities are created only by the following policy rule actions: Log Full Details With Values, and Log Full Details Per Session With Values.

| Attribute | Description                                                                                                                              |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------|
| Values    | One or more values from the logged construct.                                                                                            |
| Timestamp | The time on the DB server that the SQL was executed. Traffic must be captured with log full details policy action to see this timestamp. |

## FULL SQL Entity

Full SQL entities are created only by the following policy rule actions: Log Full Details, Log Full Details With Values, Log Full Details Per Session, or Log Full Details Per Session With Values.

| Attribute               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access Rule Description | Description of the policy rule whose action triggered the logging of the Full SQL record.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Ack Response Time       | Acknowledged Response Time in milliseconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Auto-Commit             | Entries are automatically numbered.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Bind Variables Values   | For DB2/zOS, a list of comma-separated bind variables.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Full Sql                | The logged SQL statement.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Full SQL ID             | Unique identifier for the Full SQL. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Instance ID             | Unique identifier for the Full SQL instance. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Original Timezone       | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br><br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00. This means that these events occurred 3 hours apart, but at the same respective local time (9 PM).                         |
| Records Affected        | The number of records affected for each session. On reports using this attribute, we suggest that you turn on aliases to properly display special cases such as Large Result Set or N/A.<br>Records affected only supports find statements for MongoDB, and does not support insert, update, and delete statements.                                                                                                                                                                                                                                                                                                                  |
| Records Affected (Desc) | When the Records Affected is a string value instead of a number, that string is stored here. For example: Large Result Set or N/A.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Response Length         | The length of the sniffer response for a SQL instance. Not supported for Db2 z/OS systems. For more information, see <a href="#">store log_general_response_length</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Response Time           | The response time for the request in milliseconds. When requests are monitored in network traffic, the response times are an accurate reflection of the time taken to respond to the request (Guardium timestamps both the client request and the server response).                                                                                                                                                                                                                                                                                                                                                                  |
| Returned Data           | Data returned for this request (if any, and if available).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Returned Data Count     | Number of rows returned from the SQL statement used in the policy rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Statement Type          | The type of SQL statement.<br>SQL: simple, direct SQL command, for example, typed directly into the CLI<br>RAW: PREPARE of a SQL statement for later execution, for example, conn.prepareStatement (select a from b where c=:value)<br>BIND: execution of a prepared statement including bound parameter values<br>Statement type is part of the FULL SQL entity and is only audited if you have configured Log Full Details for this statement within the policy.<br>You can not filter out specific statement types in the policy, for example, audit-only SQL and BIND statements. You can, however, filter these out in reports. |
| Succeeded               | Indicates if the call succeeded. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Timestamp               | The time when the SQL started running in the database server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## Application Events Entity

This entity is created each time that the system observes an Application Events API call (which sets these attribute values) or a stored procedure call that has been identified as a Custom Identification Procedure (which maps stored procedure parameters to these attributes).

| Attribute               | Description                                                                                                                                                                                                                                                                                 |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application Event ID    | Unique identifier for this application events entity. Only available to users with the admin role.                                                                                                                                                                                          |
| Event Date              | Datetime value, set by GuardAppEvent:Start. It displays in the format yyyy-mm-dd hh:mm:ss.<br>Note: If an attempt is made to set the event date using a format other than yyyy-mm-dd, it will contain all zeroes. The time portion (hh:mm:ss) is optional, and if omitted will be 00:00:00. |
| Event Release Date      | Datetime value, set by GuardAppEvent:Released. It displays in the format yyyy-mm-dd hh:mm:ss.                                                                                                                                                                                               |
| Event Release Type      | Type of event, set by GuardAppEvent: Released.                                                                                                                                                                                                                                              |
| Event Release User Name | User name, set by GuardAppEvent: Released.                                                                                                                                                                                                                                                  |
| Event Release Value Num | Numeric value, set by GuardAppEvent: Released.                                                                                                                                                                                                                                              |
| Event Release Value Str | String value, set by GuardAppEvent: Released.                                                                                                                                                                                                                                               |
| Event Type              | Type of event, set by GuardAppEvent:Start.                                                                                                                                                                                                                                                  |
| Event User Name         | User name, set by GuardAppEvent:Start.                                                                                                                                                                                                                                                      |
| Event Value Str         | String value, set by GuardAppEvent:Start.                                                                                                                                                                                                                                                   |
| Event Value Num         | Numeric value, set by GuardAppEvent:Start.                                                                                                                                                                                                                                                  |

| Attribute         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Original Timezone | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00. This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |
| Timestamp         | Created only once, when the event is logged. Do not confuse this attribute with the Event Date attribute, which can be set using an API call or from a stored procedure parameter. (See a description of the Application Events API in <a href="#">Identify Users with API</a> .)                                                                                                                                                                                                                                                                                                                        |

## SQL Entity

This entity is created for each unique string of SQL. Values are replaced by question marks - only the format of the string is stored.

| Attribute     | Description                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------|
| Bind Info     | Bind information for this SQL string.                                                                           |
| Construct ID  | Uniquely identifies the construct in which the SQL appeared                                                     |
| Sql           | SQL string.                                                                                                     |
| Truncated SQL | Indicates if the SQL has been truncated or not where:<br>0 - false/no, not truncated<br>1 - true/yes, truncated |

## Command Entity

For each command, an entity is created for each parent node and position in which the command appears in a command construct.

| Attribute    | Description                                                                                             |
|--------------|---------------------------------------------------------------------------------------------------------|
| Command Id   | Uniquely identifies the command. Only available to users with the admin role.                           |
| Construct Id | Uniquely identifies the construct (e.g., select a from b). Only available to users with the admin role. |
| Depth        | Depth of the command in the SQL parse tree.                                                             |
| Parent       | Identifier of parent node in the parse tree.                                                            |
| SQL Verb     | Main verb in SQL command (e.g., select, insert, delete, etc.).                                          |

## Object Command Entity

Describes an object-command entity.

| Attribute      | Description                               |
|----------------|-------------------------------------------|
| Object/Command | An object value combined with a SQL verb. |

## Object Entity

An instance of this entity is created for each object in a unique schema.

| Attribute          | Description                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------|
| App Object Module1 | Uniquely identifies the application object module.                                                                |
| Construct Id       | Uniquely identifies the construct in which the object is referenced. Only available to users with the admin role. |
| Object Id          | Uniquely identifies the object. Only available to users with the admin role.                                      |
| Object Name        | Name of the object.                                                                                               |
| Schema             | Database schema for the object.<br>Note: This attribute is deprecated since it is never populated                 |

## Join Entity

A join table is a way of implementing many-to-many relationships. Use join entity to join tables in a SELECT SQL statement.

| Attribute    | Description                                               |
|--------------|-----------------------------------------------------------|
| Construct ID | Identifies the construct in which the join is referenced. |
| Join ID      | Unique identifier                                         |
| Join SQL     | Join tables                                               |
| Timestamp    | Date and Time that the Join Entity was created.           |
| Where SQL    | Where clause (join conditions)                            |

## Field SQL Value Entity

These entities are created only by policy rule actions that log with values, for example: Log Full Details With Values, and Log Full Details Per Session With Values. The field value logged may or may not be associated with a field name. For example, field names are available (in the Field entity) if the following statement is logged:

insert into t1 (foo, bar) (10, 20)

But not available when the following statement is logged:

insert into t2 (10, 20)

| Attribute | Description                              |
|-----------|------------------------------------------|
| Value     | A field value from the logged construct. |

## Object Field Entity

---

Describes an object-field entity. Note fields with no objects will not show up in reports that include the object.

| Attribute    | Description                                  |
|--------------|----------------------------------------------|
| Object/Field | An object value combined with a field value. |

## Field Entity

---

Each time Guardium encounters a new field, it creates a field entity.

| Attribute    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Command ID   | Uniquely identifies the main command from the construct in which it was referenced. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                              |
| Construct ID | Uniquely identifies the construct in which it was referenced. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                    |
| Field ID     | Uniquely identifies the field. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Field Name   | Name of the field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| List Clause  | Use these attributes to order complex SQL queries.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Where Clause | Example of SQL queries:<br><br>Order by<br>SELECT * FROM dept_costs<br>WHERE dept_total ><br>ON Clause<br>(SELECT avg FROM avg_cost)<br>ORDER BY department<br>Having<br>SELECT column_name1, SUM(column_name2)<br>FROM table_name<br>GROUP BY column_name1<br>HAVING (numerical function condition)<br>Group By<br>SELECT column_name1, SUM(column_name2)<br>FROM table_name<br>GROUP BY column_name1<br>Where<br>SELECT FirstName, LastName, City<br>FROM Users<br>WHERE City = Los Angeles |
| Object ID    | Uniquely identifies the object from the construct in which it was referenced. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                    |

## Qualified Object Entity

---

A *tuple* allows multiple attributes to be combined together to form a single group member. In this case, the fields Server IP, Service name, DB name, DB user and Object are combined together. For more information, see [Tuple groups](#).

| Attribute        | Description                                               |
|------------------|-----------------------------------------------------------|
| Qualified Object | Tuple - Server IP, Service name, DB name, DB user, Object |

## Access Policy domain

---

Use the Access Policy domain to track all available policies on system. This topic describes the domain's entities and attributes.

Available to roles: all

## Access Policy Entity

---

Similar to the Installed Policies entity used for all installed policies on system.

| Attribute | Description |
|-----------|-------------|
|           |             |

| <b>Attribute</b>      | <b>Description</b>                                         |
|-----------------------|------------------------------------------------------------|
| Policy ID             | Uniquely identifies an access policy                       |
| Policy Description    | Describes the access policy                                |
| Selective Audit Trail | Indicates if this is a selective audit trail policy (T/F). |
| Audit Pattern         | Test pattern used for a selective audit trail policy.      |
| Timestamp             | Timestamp for the creation of the record.                  |

## Rule Entity

---

Can be used for Installed policy rule entity or access policy rule entity. There is one for each rule of the installed policy/policies or access policy/policies. Apart from the ID fields (which uniquely identify components on the internal database), all of these fields are described in the Policies help topic.

- GDM\_INSTALLED\_POLICY\_RULES\_ID - Identifies an installed policy rule.
- ACCESS\_RULE\_ID - Identifies an access rule.
- Rule Description - From the policy definition.
- Rule Position - Position within the policy.
- Rule Type - Access, Exception, or Extrusion.
- LAST\_ACCESED - Last
- Client IP - From the rule definition.
- Client Net Mask - From the rule definition.
- Client IP Group - From the rule definition.
- Server IP - From the rule definition.
- Server IP Mask - From the rule definition.
- Client MAC - From the rule definition.
- Net Protocol - From the rule definition.
- Net Protocol Group - From the rule definition.
- Field - From the rule definition.
- Field Group - From the rule definition.
- Object - From the rule definition.
- Object Group - From the rule definition.
- Command - From the rule definition.
- Command Group - From the rule definition.
- Object-Field Group - From the rule definition.
- DB Type - From the rule definition.
- Service Name - From the rule definition.
- Service Name Group - From the rule definition.
- DB Name - From the rule definition.
- DB Name Group - From the rule definition.
- DB User - From the rule definition.
- DB User Group - From the rule definition.
- App. User - From the rule definition.
- App User Group - From the rule definition.
- OS User - From the rule definition.
- OS User Group - From the rule definition.
- Src App. - From the rule definition.
- Source Program Group - From the rule definition.
- Pattern/ XML Pattern - From the rule definition.
- Period - From the rule definition.
- Min. Ct. - From the rule definition.
- Reset Interval - From the rule definition.
- Continue to next Rule/ Revoke - From the rule definition.
- Rec. Vals. - From the rule definition.
- App Event Exists - From the rule definition.
- Event Type - From the rule definition.
- App Event Text Value - From the rule definition.
- App Event Date Value - From the rule definition.
- Event User Name - From the rule definition.
- Error Code - From the rule definition.
- Exception Type - From the rule definition.
- Category Name- From the rule definition.
- Classification Name - From the rule definition.
- Severity - From the rule definition.
- Data Pattern - From the rule definition.
- SQL Pattern - From the rule definition.
- Masking Pattern - From the rule definition.
- Client IP/ Group - Provides the ability to display a single attribute and its related (if any) in a single column of the report.
- Sever IP/ Group - Provides the ability to display a single attribute and its related (if any) in a single column of the report.
- Net Protocol/ Group - Provides the ability to display a single attribute and its related (if any) in a single column of the report.
- Field Name/ Group - Provides the ability to display a single attribute and its related (if any) in a single column of the report.
- Object Name/ Group - Provides the ability to display a single attribute and its related (if any) in a single column of the report.
- Command/ Group - Provides the ability to display a single attribute and its related (if any) in a single column of the report.
- Service Name/ Group - Provides the ability to display a single attribute and its related (if any) in a single column of the report.
- DB Name/ Group - Provides the ability to display a single attribute and its related (if any) in a single column of the report.
- App. User/ Group - Provides the ability to display a single attribute and its related (if any) in a single column of the report.
- OS User/ Group - Provides the ability to display a single attribute and its related (if any) in a single column of the report.
- Source Program/ Group - Provides the ability to display a single attribute and its related (if any) in a single column of the report.
- Error Code/ Group - Provides the ability to display a single attribute and its related (if any) in a single column of the report.
- App. Event Text/ Numeric/ Date - The application events text, numeric, and date attributes.

- Category/ Classification - The combined category and classification for the rule.
- GDM\_Installed\_Policy\_Header\_ID - Identifies an installed policy header.

Note: GDM\_INSTALLED\_POLICY\_RULES\_ID and ACCESS\_RULE\_ID are available to users with the admin role only.

## Rule Action Entity

Can be used Installed policy rule action entity or access policy rule action entity. There is one for each rule of the installed policy/policies or access policy/policies .

- Sequence - Sequence of the action within the rule.
- Action
  - Block the request - See Blocking Actions in Policies.
  - Log or ignore the violation or the traffic - See Log or Ignore Actions in Policies.
  - Alert - See Alerting Actions in Policies.

## Alert Notification Entity

Describes a policy alert notification.

| Attribute               | Description                                                                     |
|-------------------------|---------------------------------------------------------------------------------|
| ALERT_NOTIFICATION_ID   | Identifies the alert notification. Only available to users with the admin role. |
| ALERT_ID                | Identifies the alert definition. Only available to users with the admin role.   |
| Alert Notification Type | Type of alert from the policy rule definition.                                  |
| Alert User              | Receiver of the alert.                                                          |
| Alert Destination       | Type of alert (EMAIL, SNMP, SYSLOG, CUSTM).                                     |
| Timestamp               | Timestamp alert record created.                                                 |

## Aggregation/Archive domain

Aggregation and archiving activity: archive, send, purge, and so on. This topic describes the domain's entities and attributes.

Available to roles: admin

## Activity Types Entity

Available only from the Aggregation/Archive domain, which by default is available to users assigned the admin role only. The Activity Types entity can be accessed only from the owning Aggregation/Import/Export Log Entity. It identifies a type of action (Prepare for Aggregation, Encrypt, Send, etc.).

| Attribute     | Description                                           |
|---------------|-------------------------------------------------------|
| Activity Type | Description of an aggregation/import/export activity. |

## Agg/Archive Log Entity

Available only from the Aggregation/Archive domain, which by default is available to users assigned the admin role only. One or more Aggregation/Import/Export Log entities are created for each activity. For example, when an aggregator system imports data, you typically see at least four activities: Prepare for Aggregation, Check Duplicate Import (one per file exported to this aggregator), Extract (one per file to be merged), Merge (one per file merged)

| Attribute          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Comment            | Additional comment for the activity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| End Time           | Ending time of activity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| File Name          | Name of file used for the activity. Files created by the archive and export operations are named as follows:<br><br><daysequence>-<scp_host>-w<run_datestamp>-d<data_date>.dbdump.enc<br><br>For example:<br><br>732423-g1.guardium.com-w20050425.040042-d2005-04-22.dbdump.enc<br><br>The date of the data contained on the file, in yyyy-mm-dd format is data_date, near the end of the file name (just before .dbdump.enc). Take care that you do not confuse this date with the run date, which appears earlier in the file name, and is the date that the data was archived or exported.                |
| Guardium Host Name | The name of the Guardium host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Original Timezone  | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br><br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00. This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |
| Period End         | Ending time for the activity being acted upon.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Period Start       | Starting time for the data being acted upon. Each archiving or aggregation activity operates on one full day of activity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Records Purged     | If the activity type is Purge, the number of records purged. Otherwise, N/A.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Status             | Status of the aggregation/import/export log activity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Start Time         | Starting time of activity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Timestamp          | Updated at the start and end of the activity being logged (prepare for archiving, encrypt, send, etc.).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Attribute | Description                               |
|-----------|-------------------------------------------|
| User Name | User name under which activity initiated. |

## Agg/Archive Debug Log Entity

| Attribute              | Description                                                                                                                                                                                           |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Aggregation Date       | Date for the data being acted upon. Each archiving or aggregation activity operates on one full day of activity.                                                                                      |
| Aggregation Duration   | Duration of the activity described by Aggregation Stage.                                                                                                                                              |
| Aggregation Exception  | If there was any exception during the activity it is presented in this field.                                                                                                                         |
| Aggregation Stage      | Stage of the aggregation activity, for example, "Initialization", "Post Purge - START"                                                                                                                |
| Aggregation Status     | Status of the Stage, for example, D: done, I: info, W: warning, E: exception                                                                                                                          |
| Aggregation Table Name | The name of the table, on which the activity is done.                                                                                                                                                 |
| Details                | Additional info, for example, "Max age is -1, age is 60. 0 days had been found"                                                                                                                       |
| Job Group              | Aggregation process name. For example:<br><br>ARCHIVE<br>ARCHIVE_RESULTS<br>CLEANUP_ORPHANS<br>DISCARD_RESULTS<br>EXPORT<br>IMPORT<br>MAINTENANCE<br>PARTITION<br>PURGE<br>RESTORE<br>RESTORE_RESULTS |
| Records Deleted        | The number of records deleted from the table described in "Aggregation Table Name" in this Aggregation Stage                                                                                          |
| Records Inserted       | The number of records inserted to the table described in "Aggregation Table Name" in this Aggregation Stage                                                                                           |
| Records Updated        | The number of records updated in the table described in "Aggregation Table Name" in this Aggregation Stage                                                                                            |
| Run Log Id             | Used Internally.                                                                                                                                                                                      |
| Timestamp              | Time when the record was inserted in the Agg/Archive Log                                                                                                                                              |

## Alert domain

This domain contains data on alerts generated and sent by Guardium. This topic describes the domain's entities and attributes.

Available to roles: all

## Activity Types Entity

Available only from the Aggregation/Archive domain, which by default is available to users assigned the admin role only. The Activity Types entity can be accessed only from the owning Aggregation/Import/Export Log Entity. It identifies a type of action (Prepare for Aggregation, Encrypt, Send, etc.).

| Attribute     | Description                                           |
|---------------|-------------------------------------------------------|
| Activity Type | Description of an aggregation/import/export activity. |

## Threshold Alert Details Entity

This entity is created each time that a correlation alert is triggered.

| Attribute         | Description                                                                                |
|-------------------|--------------------------------------------------------------------------------------------|
| Alert Log ID      | Uniquely identifies the alert details entity. Only available to users with the admin role. |
| Query Value       | Value returned by query.                                                                   |
| Base Value        | Value assigned for the statistical alert.                                                  |
| Checked From Date | The starting date and time checked for by the alert condition.                             |
| Checked To Date   | The ending date and time checked for by the alert condition.                               |
| Alert Threshold   | Alert threshold defined for the alert.                                                     |
| Notification Sent | Text of notification sent.                                                                 |
| Timestamp         | Created only once, when the statistical alert is logged.                                   |
| Alert Description | The description contained in the alert definition.                                         |

## Message Text Entity

For a threshold alert, the text of the message.

| Attribute       | Description                                          |
|-----------------|------------------------------------------------------|
| Message Text ID | Uniquely identifies the message text                 |
| Message Subject | Message subject (for an email message, for example). |
| Message Text    | Message text.                                        |

| Attribute         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Original Timezone | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00, This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |

## Messages Sent Entity

For each threshold alert message sent, the message type, recipients, status, and date of that message.

| Attribute          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Message ID         | Uniquely identifies the message                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Message Type       | Type of message.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Sent To            | One or more recipients of message.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Message Status     | Status of message:<br>FAIL The send operation failed.<br><br>WAIT The message has not yet been sent.<br><br>SENT The message was sent.                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Message Date       | Date message sent.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Message Context    | Message type:<br>INFO Informational message.<br><br>WARNING Possible error condition.<br><br>ALERT Real time or threshold alert.<br><br>ERROR Software or hardware error condition.<br><br>DEBUG Debugging message.                                                                                                                                                                                                                                                                                                                                                                                      |
| Message Originator | The module creating the message; for example monitor or GuardiumJetspeedUser.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Original Timezone  | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00, This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |

## Analytic Threat Analytics domain

This domain has detailed descriptions of active threat analytics. This topic describes the domain's entities and attributes.

Available to roles: admin

## Analytic Source Entity

This entity describes the source on which the case occurred.

| Attribute   | Description                                                 |
|-------------|-------------------------------------------------------------|
| DB User     | DB user whose actions were observed in creating this case.  |
| Database    | Database whose actions were observed in creating this case. |
| OS User     | OS User whose actions were observed in creating this case.  |
| Privileged  | Whether user is privileged or not                           |
| Server IP   | Server IP on which the actions were observed.               |
| Source Type | Source Type on which the actions were observed.             |

## Analytic Case entity

This entity describes the case details.

| Attribute              | Description                                                                                          |
|------------------------|------------------------------------------------------------------------------------------------------|
| Actual severity        | The actual severity level defined by the user. This allows the user to give feedback to the system.  |
| Actual threat category | The actual threat category defined by the user. This allows the user to give feedback to the system. |
| Case Number            | Case number assigned by Guardium®                                                                    |
| Date                   | Date case was opened                                                                                 |
| Closed by              | User name that closed the case                                                                       |
| Create Date            | Date on which Guardium created the case.                                                             |
| Originating Unit       | The unit on which the observation occurred.                                                          |
| Period Start           | The first observation occurred during the time period that started as indicated.                     |
| Severity               | Case severity assigned by Guardium: low medium, high.                                                |

| Attribute       | Description                                                                                                                                                       |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Threat Category | Type of threat, for example: anomaly, account takeover, denial of service, data tampering, schema tampering, data leak, malicious stored procedure, SQL injection |
| Timestamp       | Timestamp when Analytic Case info was last modified                                                                                                               |

## Analytic Case Observation entity

This entity describes the observations that spawned the case.

| Attribute   | Description                                       |
|-------------|---------------------------------------------------|
| Case Number | Case number assigned by Guardium                  |
| Observation | Potential attack symptoms, identified by Guardium |
| Priority    | Symptom Priority                                  |

## Analytic Outlier Details domain

This domain has detailed descriptions of activities and errors that have been identified as outliers. This topic describes the domain's entities and attributes.

Available to roles: admin

### Analytic Outlier Details Entity

| Attribute               | Description                                                                                      |
|-------------------------|--------------------------------------------------------------------------------------------------|
| Anomaly Score           | Final anomaly score                                                                              |
| Client hostname         | Client host name.                                                                                |
| Client IP               | Client IP address.                                                                               |
| DB User Name            | DB user that executed the activity.                                                              |
| Error Outlier           | Whether or not the outlier is of type error. True/False.                                         |
| High Volume Outlier     | Whether or not the outlier is of type high volume. True/False.                                   |
| New Outlier             | Whether or not the outlier is of type new. True/False.                                           |
| Number of Instances     | Activity volume.                                                                                 |
| OS User                 | OS user that executed the activity.                                                              |
| OS user                 | OS user account for the interaction.                                                             |
| Object                  | Object on which the user executed the activity.                                                  |
| Objects/Verbs           | The object/verb combination that was used in the activity.                                       |
| Outlier Type            | Deprecated                                                                                       |
| Period Start            | Start time of the period in which the activity occurred.                                         |
| Server IP               | IP of server on which the activity occurred.                                                     |
| Server Type             | Type of server on which the activity occurred.                                                   |
| Service Name            | The service name that was used in the activity.                                                  |
| Source Program          | Source Program in which the activity occurred.                                                   |
| Temp Outlier            | Whether or not the outlier is of type temp. True/False. Deprecated from v11.1.                   |
| Textual description     | Description of the outlier activity; may include, for example, database name, user name, object. |
| Timestamp               | Timestamp of the activity.                                                                       |
| Verb                    | The verb used in the activity.                                                                   |
| Vulnerable obj. Outlier | Whether or not the outlier is of type vulnerable object. True/False.                             |

## Analytic Outliers Status domain

This domain describes the outlier mining process and its results. This topic describes the domain's entities and attributes.

Available to roles: admin

### Analytic Status Entity

| Attribute                    | Description                                                          |
|------------------------------|----------------------------------------------------------------------|
| Details                      | Details related to the current status                                |
| End Analysis Time            | Time at which the analysis completed.                                |
| Number of databases analyzed | Number of DBs on which analysis was run.                             |
| Number of outliers           | Number of outliers found in the period.                              |
| Number of records analyzed   | Number of rows, after aggregation, that were analyzed in the period. |
| Number of users analyzed     | Number of users in the analysis.                                     |
| Period Analyzed              | Period start time.                                                   |

| Attribute           | Description                                                                                                                                                                                                                                                                                                             |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process name        | One of: <ul style="list-style-type: none"><li>• Reconfig: setting up parameters, or requesting information about parameters.</li><li>• Analysis: outlier mining</li><li>• Active Analytics: active threat analytics</li><li>• Enable Outlier: enabling outliers</li><li>• Disable Outlier: disabling outliers</li></ul> |
| Run by              | The user who ran the process.                                                                                                                                                                                                                                                                                           |
| Start Analysis Time | Time at which the analysis started, after receiving all the data from the collectors.                                                                                                                                                                                                                                   |
| Status              | E: Error (error listed in details); D: Done (completed successfully); P: Pending (waiting for data from collectors); R: Running; W: Warning (not a blocker).                                                                                                                                                            |
| Timestamp           | Last time at which the row was updated.                                                                                                                                                                                                                                                                                 |

## Analytic Outlier Summary domain

A summary of the outliers that occurred during the last hour on a source. This topic describes the domain's entities and attributes.

Available to roles: admin

### Analytic Outlier Summary Entity

| Attribute                           | Description                                                                                |
|-------------------------------------|--------------------------------------------------------------------------------------------|
| Alert Feedback ID                   | ID of rule that caused this feedback alert.                                                |
| Anomaly Score                       | Final anomaly score for this activity.                                                     |
| DB User Name                        | DB user that executed the activity.                                                        |
| Diverse Outlier                     | Whether or not the outlier is of type diverse. True/False.                                 |
| Error Outlier                       | Whether or not the outlier is of type error. True/False.                                   |
| High Volume Outlier                 | Whether or not the outlier is of type high volume. True / False.                           |
| New Messages Average                | Average number of new messages by the entity that caused the outlier.                      |
| New Messages Score                  | Measure of new activity abnormality.                                                       |
| New Messages SD                     | Deprecated                                                                                 |
| New Outlier                         | Whether or not the outlier is of type new outlier. True/False.                             |
| Number of Fails                     | Number of failed activities.                                                               |
| Number of New Messages              | Number of new types of new activities.                                                     |
| Number of Sensitive Objects         | Number of sensitive objects touched by in this interval.                                   |
| Number of Temporary Objects         | Number of temporary objects used in this interval.                                         |
| Number of Temporary Source Programs | Deprecated                                                                                 |
| OS User                             | OS user that executed the activity.                                                        |
| Ongoing Outlier                     | Whether or not the outlier is of type ongoing. True/False.                                 |
| Original Host Name                  | Client hostname.                                                                           |
| Outliers Summary ID                 | Unique ID.                                                                                 |
| Period Start                        | Date and time of the period start.                                                         |
| Privileged User                     | Whether or not the activity was performed by a privileged user. True/False.                |
| Rarity and Volume Score             | Deprecated                                                                                 |
| Server IP                           | IP of server on which the activity occurred.                                               |
| Server Type                         | DAM or FAM.                                                                                |
| Service Name                        | The service name that was used in the activity.                                            |
| Source ID                           | The source ID from which the activity occurred                                             |
| Temp Outlier                        | Whether or not the outlier is of type temp. True/False.                                    |
| Temporary Objects Average           | Average of above statistic in recent hours.                                                |
| Temporary Objects Score             | Measure of temporary objects usage abnormality.                                            |
| Temporary Objects SD                | Standard deviation of number of temporary objects used in this interval from recent hours. |
| Temporary Source Programs Score     | Deprecated                                                                                 |
| Timestamp                           | Timestamp of the activity.                                                                 |
| Type of Temporary Source Programs   | Deprecated                                                                                 |
| Type Volume Rarity                  | Deprecated                                                                                 |

## Application Data domain

Connection, session, and application data recorded for special non-Guardium application (Siebel and SAP, for example). This topic describes the domain's entities and attributes.

Available to roles: admin

### Client/Server Entity

This entity describes a specific client-server connection. An instance is created each time a unique set of attributes (excluding the Timestamp) is detected.

Note: For Access Tracking only, Client/Server Entity name appears in the menu as two possible entities - Client/Server and Client/Server By Session. Client/Server By Session gets its count from the Client/Server and date conditions from the Session.

Client/Server gets its count from the Client/Server and date conditions also from the Client/Server.

If you select Client/Server, then the query is populated with ATTRIBUTE\_ID = 1. If you select Client/Server By Session, then the query is populated with MAIN\_ATTRIBUTE\_ID = 0.

| Attribute                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access ID                                    | A unique identifier for this unique set of client/server connection attributes. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Analyzed Client IP                           | Applies only to encrypted traffic; when set, client IP is set to zeroes.<br>Analyzed Client IP contains the IP for encrypted sessions. For unencrypted sessions Analyzed Client IP will be the same as Client IP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Client Host Name                             | Client host name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Client IP                                    | Client IP address. For ASO traffic, CLIENT_IP is not the actual client IP; use the Analyzed Client IP, which is the correct IP. For Oracle ASO encrypted IPv6 traffic (local as well as remote), use the Client Host Name to identify the actual client session, due to limitations. For SSL traffic, Client IP is not the actual client IP and there is no Analyzed Client IP.                                                                                                                                                                                                                                                                                                                                             |
| ClientIP / DBUser                            | Paired attribute value consisting of the client IP address and database user name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Client IP/Src App/DB User/Server IP/Svc Name | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Client IP/Src App/User                       | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Client MAC                                   | Client hardware address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Client OS                                    | Client operating system.<br>For Teradata, as there is no direct information about client/server OS, instead, the data format type is used; indicating how integer data are stored during db session. This has a close relation to the platform being used and may appear as follows:<br><br>IBM MAINFRAME // IBM mainframe data format<br><br>HONEYWELL MAINFRAME // Honeywell mainframe data format<br><br>AT&T 3B2 // AT&T 3B2 data format.<br><br>INTEL 8086 // Intel 8086 data format (IBM PC or compatible)<br><br>VAX // VAX data format<br><br>AMDAHL // Amdahl data format                                                                                                                                          |
| DB Protocol                                  | Protocol specific to the database server For example, DRDA (Db2), TNS (Oracle), or TDS (MS SQL Server).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| DB Protocol Version                          | Protocol version for the DB Protocol.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| DB User Name                                 | Database user name: user that connected to the database, either local or remote.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Last Used                                    | The timestamp of the last time the data was used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Network Protocol                             | Network protocol used (such as TCP or UDP. For K-TAP on Oracle, this displays as either IPC or BEQ)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| OS User                                      | OS user as reported by the database client where supported by the database type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Server Description                           | Server description (if any). For example, displays cluster name of the Cloudera Data Platform.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Server Host Name                             | Server host name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Server IP                                    | Server IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Server IP/DB user                            | Paired attribute value consisting of Server IP address and database user name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Server IP/Svc Name/DB User                   | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Server OS                                    | Server operating system.<br>For Informix, the OS may appear as follows:<br><br>IEEEEM indicating Unix or JDBCIEEEI indicating WindowsDEC indicating DEC Alpha<br><br>For Teradata, as there is no direct information about client/server OS, instead, the data format type is used; indicating how integer data are stored during db session. This has a close relation to the platform being used and may appear as follows:<br><br>IBM MAINFRAME // IBM mainframe data format<br><br>HONEYWELL MAINFRAME // Honeywell mainframe data format<br><br>AT&T 3B2 // AT&T 3B2 data format.<br><br>INTEL 8086 // Intel 8086 data format (IBM PC or compatible)<br><br>VAX // VAX data format<br><br>AMDAHL // Amdahl data format |
| Server Type                                  | The type of database monitored, such as Dd2, Oracle, or Teradata.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Service Name                                 | Service name for the interaction. In some cases (AIX shared memory connections, for example), the service name is an alias that is used until the actual service is connected. In those cases, once the actual service is connected, a new session is started - so what the user experiences as a single session is logged as two sessions.<br>For Teradata, Service name contains the session logical host id value.                                                                                                                                                                                                                                                                                                       |
| Source Program                               | Source program as reported by the database client where supported by the database type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

| Attribute                 | Description                                                                                                                                                                                                                                                                               |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Client/ Server by session | Client/Server by session is also a Main Entity. Access this secondary entity by clicking on the Client/Server primary entity.                                                                                                                                                             |
| Timestamp                 | The time on the collector when the client <b>first</b> connected to the server. For example, if a client is connecting to the server in the same way many days in a row this timestamp will be the time of the first connection. This may even be before the purge days of the appliance. |
| Timestamp Date            | Date only from the timestamp.                                                                                                                                                                                                                                                             |
| Timestamp Time            | Time only from the timestamp.                                                                                                                                                                                                                                                             |
| Timestamp Weekday         | Weekday only from the timestamp.                                                                                                                                                                                                                                                          |
| Timestamp Year            | Year only from the timestamp.                                                                                                                                                                                                                                                             |

## Session Entity

This entity is created for each Client/Server database session.

| Attribute             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access ID             | A unique identifier for this unique set of client/server connection attributes. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Client Port           | Client port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Database Name         | Name of database for the session.<br>For Oracle, Database Name may contain additional and application specific information such as the currently executing module for a session that has been set in the MODULE column of the V\$SESSION view.                                                                                                                                                                                                                                                                                                                                                           |
| Duration (secs)       | Indicates the length of time between the Session Start and the Session End (in seconds).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Global ID             | Uniquely identifies the session - access. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Ignored Since         | Timestamp created when starting to ignore this session.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Inactive Flag         | <ul style="list-style-type: none"> <li>• -1: Session closed by timeout.</li> <li>• 0 (default): Open for sessions generated by SQL package.</li> <li>• 1: Closed (disconnect/ logout received).</li> <li>• 2: Closed due to timeout on Guardium system. The session is reopened when traffic is regenerated in the session.</li> <li>• 3: For sessions generated from non-SQL packets.</li> </ul>                                                                                                                                                                                                        |
| Old Session ID        | Points to the session from which this session was created. Zero if this is the first session of the connection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Original Timezone     | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00. This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |
| Process ID            | The process ID of the client that initiated the connection (not always available).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Server Port           | Server port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Session Encrypted     | Whether the session is encrypted. 0: no; 1: yes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Session End           | The time on the DB server when the session ended. Session End is also a Main Entity. Access this secondary entity by clicking on the Session primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Session End Date      | Date only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session End Time      | Time only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session End Weekday   | Weekday only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Session End Year      | Year only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session ID            | Uniquely identifies the session. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Session Ignored       | A Yes indicates that the session was ignored using the IGNORE SESSION policy action.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Session Start         | The time on the DB server when the session started. Session Start is also a Main Entity. Access this secondary entity by clicking on the Session primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Session Start Date    | Date only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Session Start Time    | Time only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Session Start Weekday | Weekday only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Session Start Year    | Year only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Terminal Id           | Terminal ID of the connection, used internally to resolve session information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Timestamp             | The time on the collector when the session information was most recently updated. Initially, a timestamp created for the first request on a client-server connection where there is not an active session in progress. Later, it is updated when the session is closed, or when it is marked inactive following an extended period of time with no observed activity. When tracking Session information, you are probably more interested in the Session Start and Session End attributes than the Timestamp attribute. If the session is closed it is be the same time as the Session End.              |
| Timestamp Date        | Date only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timestamp Time        | Time only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timestamp Weekday     | Weekday only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Timestamp Year        | Year only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Attribute            | Description                                                                                                                                                                                                                                                                  |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TTL                  | Only available to users with the admin role.                                                                                                                                                                                                                                 |
| Uid Chain            | For a session reported by Unix S-TAP (K-TAP mode only), or FAM on Windows, this shows the chain of OS users, when users <code>su</code> with a different user name. For more information, see <a href="#">Linux-Unix: UID chains</a> and <a href="#">UID chain for FAM</a> . |
| Uid Chain Compressed | The UID chain excluding the first user and the last user. For more information, see <a href="#">Linux-Unix: UID chains</a> and <a href="#">UID chain for FAM</a> .                                                                                                           |

## Application Data Entity

Used for the SAP and Siebel reports.

| Attribute           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application Data ID | Unique identifier for this data.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Application Code    | The application type code.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Full SQL ID         | Identifies the full SQL data.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Application Type    | Application type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| User                | Application user name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Operation Type      | The type of operation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Change Date         | Date of the change.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Time Stamp          | Time stamp for this record.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Item Name           | Name of the item affected.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Transaction Code    | Transaction code.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| System ID           | Unique identifier for the system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Record Detail 1     | Varies by item type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Record Detail 2     | Varies by item type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Record Detail 3     | Varies by item type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Record Detail 4     | Varies by item type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| VBKey               | The VBKey value.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Original Timezone   | <p>The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.</p> <p>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00. This means that these events occurred 3 hours apart, but at the same respective local time (9 PM).</p> |

## Audit Process domain

The execution of audit processes and the distribution of results. : entities and attributes

Available to roles: all

## Audit Process Entity

This entity contains basic definition parameters for an audit process.

| Attribute             | Description                                                |
|-----------------------|------------------------------------------------------------|
| Active                | Indicates if the process is active (able to be scheduled). |
| Keep Result Days      | The number of days the results are kept by the system.     |
| Keep Results Quantity | The number of results sets that are kept by the system.    |
| Process Description   | Description from audit process definition.                 |

## Audit Process Comments Entity

This entity has comments attached to an audit process definition. Comments attached to audit process results are contained the Audit Process Results Comments entity.

| Attribute                       | Description                 |
|---------------------------------|-----------------------------|
| Audit Process Comment           | The text of the comment.    |
| Audit Process Comment Creator   | The creator of the comment. |
| Audit Process Comment Timestamp | Timestamp for the comment.  |

## Audit Task Entity

This entity describes a single audit task (within an audit process).

| Attribute        | Description                                |
|------------------|--------------------------------------------|
| Task Description | Name of the task from the task definition. |

| Attribute | Description                                                                                                                                                                                                                                          |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Task Type | A numeric value indicates whether the task is a report, security assessment, entity audit trail, privacy set, or classification process. Aliases are defined for these types, so reports with Aliases on will simplify reading of the report output. |

## Audit Process Result Entity

This entity contains the execution date for a set of audit process results.

| Attribute      | Description                              |
|----------------|------------------------------------------|
| Execution Date | The date the audit process was executed. |

## Task Receiver Entity

Indicates the action required by the results receiver.

| Attribute       | Description                              |
|-----------------|------------------------------------------|
| Action Required | Indicates if signing action is required. |

## Task Results To-Do List Entity

Indicates the current status of the results.

| Attribute              | Description                                  |
|------------------------|----------------------------------------------|
| Action Required        | Indicates if signing action is required.     |
| (Esca) Action Required | Indicates if to-do list action is required.  |
| Status                 | Indicates the current status of the results. |

## User Entity

Identifies the Guardium user defined as an audit process results receiver.

| Attribute     | Description                                  |
|---------------|----------------------------------------------|
| EMAIL Address | Email address defined for the Guardium user. |
| First Name    | First name for the Guardium user.            |
| Last Active   | Timestamp for last activity for this user.   |
| Last Name     | Last name for the Guardium user.             |
| Login Name    | Guardium user name.                          |

## Audit Process Results Comments Entity

This entity has comments attached to an audit process results. Comments attached to an audit process definition are contained the Audit Process Comments entity.

| Attribute                       | Description                 |
|---------------------------------|-----------------------------|
| Audit Process Comment           | The text of the comment.    |
| Audit Process Comment Creator   | The creator of the comment. |
| Audit Process Comment Timestamp | Timestamp for the comment   |

## Auto-discovery domain

Database auto-discovery activity, including all processes that have been run, and the hosts and ports discovered. This topic describes the domain's entities and attributes.

Available to roles: all

## Auto-discovery Scan Entity

This entity identifies when a scan executed.

| Attribute         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scan Timestamp    | The time the scan executed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Original Timezone | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00. This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |

## Discovered Host Entity

This entity identifies a discovered host.

| Attribute | Description |
|-----------|-------------|
|           |             |

| Attribute         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server IP         | IP address of the discovered host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Server Host Name  | Host name of the discovered host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Original Timezone | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br><br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00, This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |

## Discovered Port Entity

This entity identifies a discovered port.

| Attribute         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port              | Discovered port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Probe Attempted   | Indicates if a probe for a supported database service has been attempted on this port. T=yes, F=no.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Port Type         | Indicates the port type (usually TCP).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| DB Type           | If a probe of the port has found a supported database type, indicates the type (DB2®, Informix®, MS SQL Server etc.)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Probe Timestamp   | The date and time that this specific port was probed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Original Timezone | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br><br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00, This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |

## BigData Intelligence Buff Usage Monitor domain

Shows the aggregate of all Sniffer Buffer Usage Entities. This topic describes the domain's entities and attributes.

Available to roles: all.

This domain is available in Guardium systems that have a defined datasource of type GBDI.

## BigData Intelligence Buff Usage Monitor Entity

| Attribute                      | Description                                                                         |
|--------------------------------|-------------------------------------------------------------------------------------|
| % CPU Mysql                    | Percentage of CPU used by MySQL.                                                    |
| % CPU Sniffer                  | Percentage of CPU used by sniffer.                                                  |
| % Mem Mysql                    | Percentage of memory used by MySQL.                                                 |
| % Mem Sniffer                  | Percentage of memory used by sniffer                                                |
| ALP                            | Analyzer Lost Packets                                                               |
| Analyzer Queue Length          | Size of the analyze queue.                                                          |
| Analyzer Rate                  | Rate at which messages are analyzed.                                                |
| DB Open FDs                    | Database open File Descriptors.                                                     |
| Eth0 Received                  | Messages received on the primary interface.                                         |
| Eth0 Sent                      | Messages sent on the primary interface.                                             |
| Extra Info                     | Internal sniffing engine data. Not usually used in queries.                         |
| Flat Log Requests              | Flat Log Requests                                                                   |
| Free Buffer Space              | Amount of free buffer space.                                                        |
| Guardium Appliance             | Host name of collector that reported this data.                                     |
| Handler Data                   | Internal sniffing engine data.                                                      |
| Logger Dbs Monitored           | List of database types currently being monitored.                                   |
| Logger Packets Ignored By Rule | Packets ignored by policy rule action.                                              |
| Logger Queue Length            | Size of logger queue.                                                               |
| Logger Rate                    | Rate at which messages are logged.                                                  |
| Logger Session Count           | Count of sessions logged.                                                           |
| Mem Sniffer                    | Amount of memory used by sniffer.                                                   |
| Mysql Disk Usage               | MySQL disk usage.                                                                   |
| Mysql Is Up                    | Boolean indicator for internal database restart (1=was restarted, 0=not restarted). |
| Open FDs                       | Open File Descriptors.                                                              |
| Promiscuous Received           | Rate of received packets through the sniffing network cards (non-interface ports).  |
| Session Direct Closed          | Count of sessions directly closed.                                                  |
| Session Guessed                | Count of sessions guessed.                                                          |
| Session Ignored                | Count of sessions ignored by sniffer.                                               |
| Session Queue Length           | Size of session queue.                                                              |
| Session Timeout                | Count of sessions timed-out.                                                        |

| Attribute                 | Description                                                                                                 |
|---------------------------|-------------------------------------------------------------------------------------------------------------|
| Session Total             | Total number of sessions.                                                                                   |
| Sessions Normal           | Count of normal sessions.                                                                                   |
| Sniffer Connections Ended | Total number of connections that were monitored and have ended since inspection engine was restarted.       |
| Sniffer Connections Used  | Total number of connections currently being monitored since inspection engine was restarted.                |
| Sniffer Packets Ignored   | Packets ignored by sniffer.                                                                                 |
| Sniffer Packets Throttled | Total number of connections that have been ignored due to throttling since inspection engine was restarted. |
| SNO                       | Session Not Opened                                                                                          |
| SPD                       | Sniffer Packets Dropped                                                                                     |
| System Cpu Load           | System CPU utilization.                                                                                     |
| System Memory Usage       | System memory utilization.                                                                                  |
| System Root Disk Usage    | System Root disk utilization.                                                                               |
| System Uptime             | Time since last start-up.                                                                                   |
| System Var Disk Usage     | System var disk utilization.                                                                                |
| TID                       | PID of sniffer process                                                                                      |
| Time Sniffer              | Elapsed time used by sniffer.                                                                               |
| Timestamp                 | Timestamp of activity                                                                                       |
| UTC Offset                | The difference in time between UTC time and time of collector that reported that data                       |
| Analyzer Queue Drops      | The number of analyzer queue entries dropped by the sniffer.                                                |
| Priority Queue Drops      | The number of priority queue entries dropped by the sniffer.                                                |

## BigData Intelligence Classification Process Log domain

Reports on classifier process logs. This topic describes the domain's entities and attributes.

Available to roles: all.

This domain is available in Guardium systems that have a defined datasource of type GBDI.

## BigData Intelligence Classification Process Log Entity

| Attribute                | Description                                                                            |
|--------------------------|----------------------------------------------------------------------------------------|
| Datasources              | Datasource list for the job.                                                           |
| Details                  | Information about the Log Event: error messages or statistics.                         |
| End Date                 | Date at end of job.                                                                    |
| End Date Time            | Timestamp at end of job.                                                               |
| Guardium Appliance       | Host name of collector that reported this data.                                        |
| Guardium Job Description | Local copy of Global Process description.                                              |
| Message                  | Information about the Log Event: error messages or statistics.                         |
| Message Type             | Type of message.                                                                       |
| Process Id               | The process ID of the client that initiated the connection (not always available).     |
| Process Run Id           | Classification process run ID.                                                         |
| Process Type             | Classification process type.                                                           |
| Queue Date               | Date in the timestamp when the job was submitted to the classifier/assessment queue.   |
| Queue Date Time          | Timestamp when the job was submitted to the classifier/assessment queue.               |
| Report Result Id         | Identifies the report result.                                                          |
| Start Date               | Date in the timestamp at start of job.                                                 |
| Start Date Time          | Timestamp at start of job.                                                             |
| Status                   | Job status.                                                                            |
| Task Description         | Name of the task from the task definition.                                             |
| UTC Offset               | The difference in time between UTC time and time of collector that reported that data. |

## BigData Intelligence Classifier Results domain

Reports on classifier process results. This topic describes the domain's entities and attributes.

Available to roles: all.

This domain is available in Guardium systems that have a defined datasource of type GBDI.

## BigData Intelligence Classifier Results Entity

| Description         | Description                       |
|---------------------|-----------------------------------|
| Catalog             | Catalog location for results set. |
| Category            | Category for the rule.            |
| Classification Name | Classification for the rule.      |

| Description            | Description                                                                           |
|------------------------|---------------------------------------------------------------------------------------|
| Column Name            | Column name from the rule definition.                                                 |
| Comments               | Any comments added to this rule definition.                                           |
| Datasource Description | Datasource for the rule.                                                              |
| Guardium Appliance     | Host name of collector that reported this data.                                       |
| Process Description    | Local copy of Global Process description                                              |
| Rule Description       | The classifier policy rule description.                                               |
| Schema                 | Schema name if applicable.                                                            |
| Start Date             | Date in the timestamp at start of job.                                                |
| Start DateTime         | Timestamp at start of job.                                                            |
| Table Name             | Table name from the rule definition.                                                  |
| UTC Offset             | The difference in time between UTC time and time of collector that reported that data |

## BigData Intelligence Databases Discovered domain

Reports on discovered databases. This topic describes the domain's entities and attributes.

Available to roles: all.

This domain is available in Guardium systems that have a defined datasource of type GBDI.

### Databases Discovered Entity

| Attribute            | Description                                                                           |
|----------------------|---------------------------------------------------------------------------------------|
| DB Type              | Type of database that was discovered.                                                 |
| Guardium Appliance   | Host name of collector that reported this data.                                       |
| Port                 | Port used when discovering the database                                               |
| Port Type            | Indicates the port type.                                                              |
| Probe Timestamp      | The date and time that this specific port was probed.                                 |
| Probe Timestamp Date | Date in the timestamp of the probe.                                                   |
| Server Host Name     | Host name of the discovered host.                                                     |
| Server IP            | IP address of the discovered host.                                                    |
| UTC Offset           | The difference in time between UTC time and time of collector that reported that data |

## BigData Intelligence Discovered Instances domain

Reports on instances that have been discovered by GIM. This topic describes the domain's entities and attributes.

Available to roles: all.

This domain is available in Guardium systems that have a defined datasource of type GBDI.

### BigData Discovered Instances Entity

| Attribute                      | Description                                                                           |
|--------------------------------|---------------------------------------------------------------------------------------|
| Client                         | IP address/mask of client                                                             |
| DB Install Dir                 | Database Install Directory                                                            |
| DB2 Shared Mem Adjustment      | Packet header size                                                                    |
| DB2 Shared Mem Client Position | Client I/O area offset                                                                |
| DB2 Shared Mem Size            | DB2 shared memory segment size                                                        |
| Exclude Client                 | IP address/mask of clients to exclude                                                 |
| Guardium Appliance             | Host name of collector that reported this data.                                       |
| Host                           | Host name for this instance                                                           |
| Informix Version               | Informix version                                                                      |
| Instance name                  | Name of the discovered instance                                                       |
| KTAP DB Port                   | Database port for KTAP                                                                |
| Named Pipe                     | Pipe name used by database                                                            |
| Port Max                       | Port range, maximum port number for inspection-engines                                |
| Port Min                       | Port range, minimum port number for inspection-engines                                |
| Proc Name                      | Process name                                                                          |
| Proc Names                     | Name of database executable                                                           |
| Protocol                       | Protocol specific to this instance                                                    |
| Timestamp                      | Timestamp created when Guardium recorded this instance of the entity.                 |
| Timestamp Date                 | Date in the timestamp                                                                 |
| Unix Socket                    | Unix Socket                                                                           |
| UTC Offset                     | The difference in time between UTC time and time of collector that reported that data |

## BigData Intelligence Exception domain

All of the exceptions and exception-related data. These are SQL exceptions sent from a database server and collected by inspection engines, as well as exceptions generated by Guardium itself. This topic describes the domain's entities and attributes.

Available to roles: all.

This domain is available in Guardium systems that have a defined datasource of type GBDI.

### BigData Exception Entity

| Attribute                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Analyzed Client IP                           | Applies only to encrypted traffic; when set, client IP is set to zeroes.<br>Analyzed Client IP has a map for CEF source. If the query used for the CEF does NOT contain the Client IP but contains the analyzed client IP, the analyzed client IP will be used for the source. If both included in the query, then Client IP takes precedence.                                                                              |
| App User Name                                | Application user name.                                                                                                                                                                                                                                                                                                                                                                                                      |
| Client Host Name                             | Client hostname                                                                                                                                                                                                                                                                                                                                                                                                             |
| Database Error Text                          | A database error code followed by a short text description of the error. The error code is taken from the Exception Description attribute of the Exception entity. Using the error code as a key, the error text is obtained from an internal table on the Guardium appliance, which contains the most common error messages (about 54,000 of them).<br>Example: ORA-00942: table or view does not exist                    |
| Database Name                                | Database Name                                                                                                                                                                                                                                                                                                                                                                                                               |
| Database Protocol                            | Database protocol for the exception.                                                                                                                                                                                                                                                                                                                                                                                        |
| DB User Name                                 | The DB user that connected to the database, either local or remote.                                                                                                                                                                                                                                                                                                                                                         |
| Description                                  | For a database exception, this is an error code from the database management system. For most common messages (about 54,000 of them), a longer text description is available in the Database Error Text attribute. That text comes from the internal Guardium database table of error messages, not from the exception itself.                                                                                              |
| Destination Address                          | Destination IP address.                                                                                                                                                                                                                                                                                                                                                                                                     |
| Error Code                                   | The database error code.                                                                                                                                                                                                                                                                                                                                                                                                    |
| Exception Date                               | Date only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                               |
| Exception ID                                 | Uniquely identifies the exception.                                                                                                                                                                                                                                                                                                                                                                                          |
| Exception Timestamp                          | Date and time when this Exception entity was logged.                                                                                                                                                                                                                                                                                                                                                                        |
| Exception Type                               | Uniquely identifies the exception type.                                                                                                                                                                                                                                                                                                                                                                                     |
| Guardium Appliance                           | Host name of collector that reported this data.                                                                                                                                                                                                                                                                                                                                                                             |
| Link to more information about the exception | Link that is sometimes available, depending on the exception source.                                                                                                                                                                                                                                                                                                                                                        |
| OS User                                      | OS user account for the interaction                                                                                                                                                                                                                                                                                                                                                                                         |
| Server Host Name                             | Server Host Name                                                                                                                                                                                                                                                                                                                                                                                                            |
| Server IP                                    | Server IP address                                                                                                                                                                                                                                                                                                                                                                                                           |
| Server Port                                  | Server port number                                                                                                                                                                                                                                                                                                                                                                                                          |
| Server Type                                  | DB2, Oracle, Sybase, and so on.                                                                                                                                                                                                                                                                                                                                                                                             |
| Service Name                                 | Service name for the interaction. In some cases (AIX® shared memory connections, for example), the service name is an alias that is used until the actual service is connected. In those cases, once the actual service is connected, a new session is started - so what the user experiences as a single session will be logged as two sessions.<br>For Teradata, Service name contains the session logical host ID value. |
| Session Id                                   | Uniquely identifies the session                                                                                                                                                                                                                                                                                                                                                                                             |
| Source Address                               | Source IP address of the exception.                                                                                                                                                                                                                                                                                                                                                                                         |
| Source Program                               | Source program for the interaction                                                                                                                                                                                                                                                                                                                                                                                          |
| SQL string that caused the Exception         | The SQL string that caused the exception.                                                                                                                                                                                                                                                                                                                                                                                   |
| User Name                                    | Database user name.                                                                                                                                                                                                                                                                                                                                                                                                         |
| UTC Offset                                   | The difference in time between UTC time and time of collector that reported that data                                                                                                                                                                                                                                                                                                                                       |

## BigData Intelligence Full SQL domain

You can create full SQL entities by using only the following policy rule actions: Log Full Details, Log Full Details With Values, Log Full Details Per Session, or Log Full Details Per Session With Values.

Available to roles: all.

This domain is available in Guardium systems that have a defined datasource of type GBDI.

### BigData Intelligence Full SQL Entity

Table 1. The following table describes the domain's entities and attributes.

| Attribute          | Description                                                                                                                                                                                                                                                                                                                              |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Analyzed Client IP | Applies only to encrypted traffic; when set, client IP is set to zeros.<br>Analyzed Client IP has a map for CEF source. If the query used for the CEF does NOT contain the Client IP but contains the analyzed client IP, the analyzed client IP is used for the source. If both included in the query, then Client IP takes precedence. |
| Client Host Name   | Client hostname                                                                                                                                                                                                                                                                                                                          |
| Database Name      | Database name                                                                                                                                                                                                                                                                                                                            |
| DB User Name       | Database username                                                                                                                                                                                                                                                                                                                        |
| Full Sql           | Full SQL statement with values.                                                                                                                                                                                                                                                                                                          |
| Guardium Appliance | Hostname of the collector that reported this data.                                                                                                                                                                                                                                                                                       |
| Instance ID        | Unique identifier for the Full SQL instance.                                                                                                                                                                                                                                                                                             |
| Network Protocol   | Network Protocol                                                                                                                                                                                                                                                                                                                         |
| OS User            | OS User                                                                                                                                                                                                                                                                                                                                  |
| Records Affected   | The number of records affected for each session. For reports that use this attribute, it's recommended to turn on aliases to properly display special cases such as Large Result Set or N/A.                                                                                                                                             |
| Response Time      | The response time for the request in milliseconds. When you monitor requests in network traffic, the response times accurately reflect the time that is taken to respond to the request (Guardium timestamps both the client request and the server response).                                                                           |
| Server Host Name   | Server hostname                                                                                                                                                                                                                                                                                                                          |
| Server IP          | Server IP                                                                                                                                                                                                                                                                                                                                |
| Server Port        | Server port                                                                                                                                                                                                                                                                                                                              |
| Server Type        | Server type                                                                                                                                                                                                                                                                                                                              |
| Service Name       | Service name                                                                                                                                                                                                                                                                                                                             |
| Session Id         | The numeric key value that Guardium assigns to uniquely identify a session. It is used to search the activities generated during the session.                                                                                                                                                                                            |
| Source Program     | Source Program                                                                                                                                                                                                                                                                                                                           |
| Succeeded          | Indicates whether the call succeeded.                                                                                                                                                                                                                                                                                                    |
| Timestamp          | The time when the SQL was executed in the database server.                                                                                                                                                                                                                                                                               |
| UTC Offset         | The difference in time between Coordinated Universal Time (UTC) time and the time of the collector that reported that data.                                                                                                                                                                                                              |

## BigData Intelligence Installed Patches domain

Reports on installed patches. This topic describes the domain's entities and attributes.

Available to roles: all.

This domain is available in Guardium systems that have a defined datasource of type GBDI.

## BigData Intelligence Installed Patches Entity

| Attribute           | Description                                                                           |
|---------------------|---------------------------------------------------------------------------------------|
| Creation Date       | The patch creation date.                                                              |
| Guardium Appliance  | Host name of collector that reported this data.                                       |
| Guardium Version    | Guardium software version                                                             |
| Installed By        | CM, SA, or CLI                                                                        |
| Patch Dependencies  | Guardium version or patch, which has to be installed before this patch.               |
| Patch Description   | Patch Description                                                                     |
| Patch Number        | Patch Number                                                                          |
| Requested Date Time | The date/time the patch should be installed                                           |
| Status              | 0/1 for success or failure                                                            |
| Status Description  | Patch                                                                                 |
| Timestamp           | Timestamp the status was updated.                                                     |
| Upload Date         | The date the patch was uploaded for installation                                      |
| UTC Offset          | The difference in time between UTC time and time of collector that reported that data |

## BigData Intelligence Instance domain

This domain contains traffic data collected by the inspection engines every time a request is sent to a server being monitored. It includes all of the client/server, session, SQL, and access periods related data. This topic describes the domain's entities and attributes.

Available to roles: all.

This domain is available in Guardium systems that have a defined datasource of type GBDI.

## BigData Intelligence Instance Entity

| Attribute               | Description                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access Rule Description | Description from the access policy rule definition.                                                                                                                                                                                                                                                                                                                                                                   |
| Analyzed Client IP      | Applies only to encrypted traffic; when set, client IP is set to zeroes.<br>Analyzed Client IP has a map for CEF source. If the query used for the CEF does NOT contain the Client IP but contains the analyzed client IP, the analyzed client IP will be used for the source. If both included in the query, then Client IP takes precedence.                                                                        |
| App User Name           | Unique identifier for this App User Name entity.                                                                                                                                                                                                                                                                                                                                                                      |
| Application Event ID    | Unique identifier for this application events entity.                                                                                                                                                                                                                                                                                                                                                                 |
| Average Execution Time  | The average command execution time during the period. This is for SQL statements only. It does not apply to FTP traffic.                                                                                                                                                                                                                                                                                              |
| Client Host Name        | Client Host Name                                                                                                                                                                                                                                                                                                                                                                                                      |
| Construct Id            | Uniquely identifies the construct in which the object is referenced.                                                                                                                                                                                                                                                                                                                                                  |
| Database Name           | Name of database for the session (MSSQL or Sybase only).<br>For Oracle, Database Name may contain additional and application specific information such as the currently executing module for a session that has been set in the MODULE column of the V\$SESSION view.                                                                                                                                                 |
| DB User Name            | User that connected to the database, either local or remote.                                                                                                                                                                                                                                                                                                                                                          |
| Failed Sqls             | The number of failed SQL requests. Appears only when the main entity for the query permits this level of detail. Not available if either Client/Server or Session is the main entity.                                                                                                                                                                                                                                 |
| Guardium Appliance      | Host name of collector that reported this data.                                                                                                                                                                                                                                                                                                                                                                       |
| Instance ID             | Unique identifier for the instance of a construct or SQL instance. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                       |
| Network Protocol        | Network protocol used (for example, TCP, UDP, etc. For K-TAP on Oracle, this displays as either IPC or BEQ).                                                                                                                                                                                                                                                                                                          |
| Objects and Verbs       | Name of the object and SQL verb tuples separated by semi colon.                                                                                                                                                                                                                                                                                                                                                       |
| Original SQL            | original SQL sent by user.                                                                                                                                                                                                                                                                                                                                                                                            |
| OS User                 | OS user account for the interaction.                                                                                                                                                                                                                                                                                                                                                                                  |
| Period Start            | Period start attribute.                                                                                                                                                                                                                                                                                                                                                                                               |
| Period Start Date       | Date only from the period start attribute.                                                                                                                                                                                                                                                                                                                                                                            |
| Server Host Name        | Server Host Name                                                                                                                                                                                                                                                                                                                                                                                                      |
| Server IP               | Server IP address                                                                                                                                                                                                                                                                                                                                                                                                     |
| Server Port             | Server port number                                                                                                                                                                                                                                                                                                                                                                                                    |
| Server Type             | For example: DB2, Oracle, Sybase...                                                                                                                                                                                                                                                                                                                                                                                   |
| Service Name            | Service name for the interaction. In some cases (AIX shared memory connections, for example), the service name is an alias that is used until the actual service is connected. In those cases, once the actual service is connected, a new session is started - so what the user experiences as a single session is logged as two sessions.<br>For Teradata, Service name contains the session logical host id value. |
| Session Id              | Uniquely identifies the session. Available only to users with the admin role.                                                                                                                                                                                                                                                                                                                                         |
| Source Program          | Source program for the interaction.                                                                                                                                                                                                                                                                                                                                                                                   |
| Successful Sqls         | The number of successful SQL requests. Appears only when the main entity for the query permits this level of detail. These are not available if either Client/Server or Session is the main entity.                                                                                                                                                                                                                   |
| Timestamp               | Timestamp this record was created.                                                                                                                                                                                                                                                                                                                                                                                    |
| Timestamp Date          | Date in the timestamp                                                                                                                                                                                                                                                                                                                                                                                                 |
| Total Records Affected  | The total number of records affected. Appear only when the main entity for the query permits this level of detail. These are not available if either Client/Server or Session is the main entity.                                                                                                                                                                                                                     |
| UTC Offset              | The time difference between UTC time and time of the collector that reported that data.                                                                                                                                                                                                                                                                                                                               |

## BigData Intelligence Outliers List Enhanced domain

Detailed description of activities and errors that have been identified as outliers. This topic describes the domain's entities and attributes.

Available to roles: all.

This domain is available in Guardium systems that have a defined datasource of type GBDI.

## BigData Intelligence Outliers List Enhanced Entity

| Attribute           | Description                                                    |
|---------------------|----------------------------------------------------------------|
| Anomaly Score       | Final anomaly score.                                           |
| DB Name             | Name of DB on which the activity occurred.                     |
| DB User Name        | DB User Name associated with the activity.                     |
| Error Outlier       | Whether or not the outlier is of type error. True/False.       |
| Guardium Appliance  | Host name of collector that reported this data.                |
| High volume Outlier | Whether or not the outlier is of type high volume. True/False. |
| New Outlier         | Whether or not the outlier is of type new. True/False.         |
| Number of Instances | Activity volume.                                               |

| Attribute         | Description                                                                           |
|-------------------|---------------------------------------------------------------------------------------|
| Object            | The object on which the activity was performed.                                       |
| Period Start      | Time of period start                                                                  |
| Period Start Date | Date of period start.                                                                 |
| Records Affected  | The number of records affected by the activity.                                       |
| Server IP         | IP of server on which the activity occurred.                                          |
| Server Type       | Type of server on which the activity occurred.                                        |
| Source Program    | Source program associated with the activity.                                          |
| Temp Outlier      | Whether or not the outlier is of type temp. True/False.                               |
| UTC Offset        | The difference in time between UTC time and time of collector that reported that data |
| Verb              | Verb used in the activity.                                                            |

## BigData Intelligence Outliers Summary Enhanced domain

A summary of the outliers on a one hour granularity. This topic describes the domain's entities and attributes.

Available to roles: all.

This domain is available in Guardium systems that have a defined datasource of type GBDI.

## BigData Intelligence Outliers Summary Enhanced Entity

| Attribute           | Description                                                                            |
|---------------------|----------------------------------------------------------------------------------------|
| Anomaly Score       | Final anomaly score for this alert.                                                    |
| DB Name             | Name of DB on which the activity occurred.                                             |
| DB User Name        | DB User Name associated with the activity.                                             |
| Diverse Outlier     | Whether or not the outlier is of type diverse. True/False.                             |
| Error Outlier       | Whether or not the outlier is of type error. True/False.                               |
| Guardium Appliance  | Host name of collector that reported this data.                                        |
| High volume Outlier | Whether or not the outlier is of type high volume. True/False.                         |
| New Outlier         | Whether or not the outlier is of type new. True/False.                                 |
| Ongoing Outlier     | Whether or not the outlier is of type ongoing. True/False.                             |
| Period Start        | Date and time of period start.                                                         |
| Period Start Date   | Date of period start.                                                                  |
| Privileged User     | Whether or not the activity was performed by a privileged user. True/False.            |
| Server IP           | IP of server on which the activity occurred.                                           |
| Server Type         | Type of server on which the activity occurred.                                         |
| Temp Outlier        | Whether or not the outlier is of type temp. True/False.                                |
| UTC Offset          | The difference in time between UTC time and time of collector that reported that data. |

## BigData Intelligence Policy Violations domain

All policy violation data, for all violations of the policy detected by the Guardium inspection engines or STAPs. This topic describes the domain's entities and attributes. This topic describes the domain's entities and attributes.

This entity is created each time that a policy rule violation is logged. Not all policy rule violations are logged - see the description of the rule actions in [Policy rule actions](#). The access rule causing the violation is available in the dependent Access Rule Entity (described earlier).

Available to roles: all.

This domain is available in Guardium systems that have a defined datasource of type GBDI.

## BigData Intelligence Policy Violations Entity

| Attribute               | Description                                                                                                                                                                                                                                                                                                                                    |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access Rule Description | The description of the rule from its definition.                                                                                                                                                                                                                                                                                               |
| Analyzed Client IP      | Applies only to encrypted traffic; when set, client IP is set to zeroes.<br>Analyzed Client IP has a map for CEF source. If the query used for the CEF does NOT contain the Client IP but contains the analyzed client IP, the analyzed client IP will be used for the source. If both included in the query, then Client IP takes precedence. |
| Client Host Name        | Client Host Name                                                                                                                                                                                                                                                                                                                               |
| DB User Name            | Database user name. The user that connected to the database, either local or remote.                                                                                                                                                                                                                                                           |
| Full SQL String         | SQL string that caused the policy rule violation.                                                                                                                                                                                                                                                                                              |
| Guardium Appliance      | Host name of collector that reported this data.                                                                                                                                                                                                                                                                                                |
| Objects and Verbs       | Database user name. The DB user name is the person who connected to the database, either local or remote.                                                                                                                                                                                                                                      |

| Attribute        | Description                                                                                 |
|------------------|---------------------------------------------------------------------------------------------|
| OS User          | OS user that caused the policy rule violation.                                              |
| Server Host Name | Server on which the policy rule violation occurred.                                         |
| Server IP        | Server IP on which the policy rule violation occurred.                                      |
| Server Type      | Server type on which the policy rule violation occurred.                                    |
| Service Name     | Service Name in which the policy rule violation occurred.                                   |
| Severity         | Severity of the policy rule violation.                                                      |
| Source Program   | Source Program in which the policy rule violation occurred.                                 |
| Timestamp        | Created when the policy rule violation is logged. Not all policy rule violations are logged |
| Timestamp Date   | Date in the timestamp                                                                       |
| UTC Offset       | The difference in time between UTC time and time of collector that reported that data       |
| Violation Log Id | Unique identifier of the violation log                                                      |

## BigData Intelligence Session domain

Reports on Client/Server database session. This topic describes the domain's entities and attributes.

Available to roles: all.

This domain is available in Guardium systems that have a defined datasource of type GBDI.

## BigData Intelligence Session Entity

| Attribute          | Description                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access Id          | Uniquely identifies the access period.                                                                                                                                                                                                                                                                                                                                                                                 |
| Analyzed Client IP | Applies only to encrypted traffic; when set, client IP is set to zeroes.<br>Analyzed Client IP has a map for CEF source. If the query used for the CEF does NOT contain the Client IP but contains the analyzed client IP, the analyzed client IP is used for the source. If both are included in the query, then the Client IP takes precedence.                                                                      |
| Client Host Name   | Client Host Name                                                                                                                                                                                                                                                                                                                                                                                                       |
| Client Port        | Client port number                                                                                                                                                                                                                                                                                                                                                                                                     |
| Database Name      | Name of database for the session (MSSQL or Sybase only).<br>For Oracle, Database Name may contain additional and application specific information such as the currently executing module for a session that has been set in the MODULE column of the V\$SESSION view.                                                                                                                                                  |
| DB User Name       | User that connected to the database, either local or remote.                                                                                                                                                                                                                                                                                                                                                           |
| Guardium Appliance | Host name of collector that reported this data.                                                                                                                                                                                                                                                                                                                                                                        |
| Ignored Flag       |                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Login Succeeded    |                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Network Protocol   | Network protocol used (for example, TCP, UDP. For K-TAP on Oracle, this displays as either IPC or BEQ).                                                                                                                                                                                                                                                                                                                |
| OS User            | OS user account for the interaction.                                                                                                                                                                                                                                                                                                                                                                                   |
| Sender IP          | Sender IP                                                                                                                                                                                                                                                                                                                                                                                                              |
| Server Host Name   | Server Host Name                                                                                                                                                                                                                                                                                                                                                                                                       |
| Server IP          | Server IP                                                                                                                                                                                                                                                                                                                                                                                                              |
| Server Port        | Server port number                                                                                                                                                                                                                                                                                                                                                                                                     |
| Server Type        | For example: DB2, Oracle, Sybase...                                                                                                                                                                                                                                                                                                                                                                                    |
| Service Name       | Service name for the interaction. In some cases (AIX® shared memory connections, for example), the service name is an alias that is used until the actual service is connected. In those cases, once the actual service is connected, a new session is started - so what the user experiences as a single session is logged as two sessions.<br>For Teradata, Service name contains the session logical host id value. |
| Session End        | Date and time the session ended. Session End is also a Main Entity. Access this secondary entity by clicking on the Session primary entity.                                                                                                                                                                                                                                                                            |
| Session End Date   | Date only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                        |
| Session ID         | Uniquely identifies the session.                                                                                                                                                                                                                                                                                                                                                                                       |
| Session Ignored    | Indicates whether or not some part of the session was ignored (beginning at any point in time).                                                                                                                                                                                                                                                                                                                        |
| Session Start      | Date and time session started. Session Start is also a Main Entity. Access this secondary entity by clicking on the Session primary entity.                                                                                                                                                                                                                                                                            |
| Session Start Date | Date only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                      |
| Source Program     | Source program for the interaction.                                                                                                                                                                                                                                                                                                                                                                                    |
| Uid Chain          | For a session reported by Unix S-TAP (K-Tap mode only), this shows the chain of OS users, when users su with a different user name. The values that appear here vary by OS platform; for example, under AIX the string IBM IBM IBM may appear as a prefix.<br>For Solaris Zones, user ids may be reported instead of user names in the Uid Chain.                                                                      |
| UTC Offset         | The time difference between UTC time and the time of the collector that reported that data.                                                                                                                                                                                                                                                                                                                            |

## BigData Intelligence STAP Status domain

Reports on status of S-TAPs. This topic describes the domain's entities and attributes.

Available to roles: all.

This domain is available in Guardium systems that have a defined datasource of type GBDI.

### BigData Intelligence STAP Status Entity

| Attribute                    | Description                                                                                |
|------------------------------|--------------------------------------------------------------------------------------------|
| App Server                   | Whether or not an App server is installed. Yes / No.                                       |
| CAS Server Name              | Name of the CAS server.                                                                    |
| DB Port max                  | Ending port number of the range of listening ports for the database.                       |
| DB Port min                  | Starting port number of the range of listening ports for the database.                     |
| DB Server Type               | Protocol of the DB server.                                                                 |
| DB Tee Real DB Port          | The port to which S-TAP forwards traffic when using Tee.                                   |
| Encrypted?                   | Whether or not communication from S-TAP is encrypted. Unencrypted / encryption type.       |
| Guardium Appliance           | Name of the collector that reported this data.                                             |
| Guardium Hosts               | IP addresses or hostnames of the Guardium systems that act as the host/s for the S-TAP.    |
| Hunter DBS                   | Deprecated                                                                                 |
| I Name                       |                                                                                            |
| KTAP                         | Whether or not K-TAP is installed on the S-TAP. Yes / No.                                  |
| KTAP Version                 | Version of the installed K-TAP.                                                            |
| Last Response Received       | Last status response received from the S-TAP. For example synchronizing, active.           |
| Last Response Time           | Time of the last status response.                                                          |
| LHMON                        | Deprecated in v10.5. Whether or not LHMON driver is installed.                             |
| MSS Shm                      | Shared Memory Driver Installed. Yes / No.                                                  |
| Pipes                        | Whether or not a named pipes driver is installed on the S-TAP. Yes / No.                   |
| Policy                       |                                                                                            |
| Primary Host Name            | Name of the Guardium appliance to which the S-TAP sends data.                              |
| STAP Changed                 |                                                                                            |
| S-TAP Host                   | IP address or hostname for the database server system on which S-TAP is installed          |
| STAP Verification Status     | Verification not run / Verification run                                                    |
| S-TAP Version                | Version of the S-TAP software                                                              |
| Status                       | S-TAP status. One of:Active, Inactive, Synchronizing.                                      |
| Tap Identifier               | Unique inspection engine identifier.                                                       |
| TAP IP                       | IP address for the database server system on which S-TAP is installed.                     |
| TAP Type                     | The type of installed S-TAP agent:<br>stap=UNIX<br><br>wstab = Windows<br>ztap=Z/OS        |
| TEE                          | Deprecated. Whether or not Tee is enabled. Yes / No.                                       |
| Time Differential            |                                                                                            |
| Timestamp                    |                                                                                            |
| Total Bytes Dropped So Far   | Total Bytes Dropped So Far                                                                 |
| Total Bytes Ignored          | Total Bytes Ignored                                                                        |
| Total Bytes So Far           | Total Bytes So Far                                                                         |
| Total Response Bytes Ignored | Total Response Bytes Ignored                                                               |
| Use TLS                      | Encrypted with TLS. Yes / No.                                                              |
| UTC Offset                   | The difference in time between UTC time and time of the collector that reported that data. |

## BigData Intelligence System Info domain

Available to roles: all.

This domain is available in Guardium systems that have a defined datasource of type GBDI. This topic describes the domain's entities and attributes.

### BigData Intelligence System Info Entity

| Attribute                | Description                                                |
|--------------------------|------------------------------------------------------------|
| Archive at Age           | Age of data, in days, at which it is archived.             |
| Archive Destination Dir  | Target location of archive operation.                      |
| Archive Destination Host | Target host of archive operation: IP or hostname.          |
| Archive Destination User | User that has read/write credentials for target directory. |
| Archive Max Age          | Maximum age of data that is archived, in days.             |

| Attribute               | Description                                                                                  |
|-------------------------|----------------------------------------------------------------------------------------------|
| Archive Selected        |                                                                                              |
| Archive Values          | Whether or not archived data includes SQL strings (yes), or are replaced with "?" (no).      |
| Auth LDAP Type          |                                                                                              |
| Auth Server Type        |                                                                                              |
| Export at Age           | Age of data, in days, at which it is exported.                                               |
| Export Destination Host | Target location of export operation.                                                         |
| Export Max Age          | Maximum age of data that is exported, in days.                                               |
| Export Selected         |                                                                                              |
| Export Values           | Whether or not exported data includes SQL strings (yes), or are replaced with ? (no).        |
| gid                     | The same as Global ID.                                                                       |
| Global ID               | Global ID.                                                                                   |
| Guardium Appliance      | Host name of collector that archived/exported this data.                                     |
| Guardium Model          | Model of host.                                                                               |
| Guardium Version        | Version of host.                                                                             |
| Host Mac Address        | Host Mac Address                                                                             |
| Import Selected         |                                                                                              |
| Manager IP              | IP Address of the unit's Central Manager.                                                    |
| Purge at Age            | Age of data, in days, at which data is purged.                                               |
| Purge if Archived       | Data is purged                                                                               |
| Purge if Exported       |                                                                                              |
| Purge Selected          |                                                                                              |
| Restore Selected        |                                                                                              |
| System Domain           |                                                                                              |
| Timestamp               | Date and time this change record was created on the server (Guardium appliance server clock) |
| Tomcat Hostname         | System Hostname                                                                              |
| Tomcat IP               | System IP Address                                                                            |
| Unique ID Prefix        | Unique Global Identifier                                                                     |
| Unit Type               | Unit type, for example, standalone, managed, manager, aggregator.                            |
| UTC Offset              | The difference in time between UTC time and time of collector that reported that data        |

## BigData Intelligence VA Results domain

Available to roles: all.

This domain is available in Guardium systems that have a defined datasource of type GBDI. This topic describes the domain's entities and attributes.

### BigData Intelligence VA Results Entity

| Attribute              | Description                                                                                    |
|------------------------|------------------------------------------------------------------------------------------------|
| Assessment Description | Assessment name from the definition.                                                           |
| Category               | Category for the test result.                                                                  |
| Datasource Name        | Name of the datasource.                                                                        |
| Datasource Type        | Database type, for example: Oracle, MS-SQL, DB2, Sybase, Informix...                           |
| DB Name                | Database name                                                                                  |
| Description            | Datasource description.                                                                        |
| Execution Date         | Date that the assessment was run.                                                              |
| Guardium Appliance     | Host name of collector that reported this data.                                                |
| Host                   | Host name of the datasource.                                                                   |
| Patch Level            | Patch level of the datasource.                                                                 |
| Port                   | Port number on the host.                                                                       |
| Recommendation         | Recommendation returned for the task.                                                          |
| Result Text            | Text returned by the test.                                                                     |
| Score Description      | Description of the score.                                                                      |
| Service Name           | Service name for the datasource.                                                               |
| Severity               | Severity of the incident or policy violation. One of: INFO, LOW, MED, HIGH.                    |
| Test Description       | Description from the test definition.                                                          |
| Test Score             | Returned test score.                                                                           |
| UTC Offset             | The difference in time between UTC time and the time of the collector that reported that data. |
| Version Level          | Version level of the database.                                                                 |

## CAS Changes domain

Tracks changes to monitored items (files, registry variables, etc.). This topic describes the domain's entities and attributes.

Available to roles: all

## Monitored Changes Entity

This entity is created each time a monitored item changes. It identifies the monitored item within the CAS instance, and points to the saved data for the change.

| Attribute             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Change Identifier     | Unique identifier for the change.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Sample Time           | Timestamp (date and time on host) that sample was taken.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Audit Config Id       | Identifies the host configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Saved Data Id         | Identifies the Saved Data entity for this change.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Audit State Label Id  | Identifies the Host Configuration entity for this change.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timestamp             | Date and time this change record was created on the server (Guardium appliance server clock).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| MD5                   | Indicates whether or not the comparison is done by calculating a checksum using the MD5 algorithm and comparing that value with the value calculated the last time the item was checked. The default is to not use MD5. If MD5 is used but the size of the raw data is greater than the MD5 Size Limit configured for the CAS host, the MD5 calculation and comparison will be skipped. Regardless of whether or not MD5 is used, both the current value of the last modified timestamp for the item and the size of the item are compared with the values saved the last time the item was checked. |
| Owner                 | Unix only. If the item type is a file, the file owner.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Permissions           | Unix only. If the item type is a file, the file permissions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Size                  | File size, but there are special values as follows:<br>-1 = File exists, but has a zero bytes<br><br>0 (zero) = File does not exist, but this file name is being monitored (it never existed or may have been deleted)                                                                                                                                                                                                                                                                                                                                                                               |
| Last Modified         | Timestamp for the last modification, taken from the file system at the sample time..                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Last Modified Date    | Date for the last modification.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Last Modified Time    | Time for the last modification.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Last Modified Weekday | Day of week for the last modification.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Last Modified Year    | Year for the last modification.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Group                 | Unix only. If the item type is a file, the group owner.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## Host Configuration Entity

A Host Configuration entity is created for each item in a CAS instance.

| Attribute            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Audit State Label Id | Unique numeric identifier for the configuration item                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Timestamp            | Timestamp for creation of the entity                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Host Name            | Database server host name or IP address                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| OS Type              | Operating system: Unix or Windows                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| DB Type              | Database type: Oracle, MS-SQL, DB2®, Sybase, Informix®, or N/A if the change is to an operating system instance                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Instance Name        | Name of the template set instance                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Type                 | Type of monitored item that changed.<br><br>OS Script or SQL Script: A change triggered by the OS script contained in the monitored item template definition.<br><br>Environment Variable: An environment variable (Unix only)<br><br>Registry Variable: A registry variable (Windows only)<br><br>File: A specific file. There is no host configuration entity for a file pattern defined in the template set used by the instance. Instead, there is a separate host configuration entity for each file that matches the pattern. |
| Monitored Item       | The name of the changed item, from the Description (if entered), otherwise a default name depending on the Type (a file name, for example).                                                                                                                                                                                                                                                                                                                                                                                         |

## Saved Data Entity

A Saved Data entity is created each time a change is detected for an item being monitored, if the Keep data box is marked for that item in the item template definition.

| Attribute         | Description                                                                   |
|-------------------|-------------------------------------------------------------------------------|
| Saved Data ID     | Unique numeric identifier for the saved data item.                            |
| Saved Data        | The actual data saved.                                                        |
| Timestamp         | Timestamp for when the saved data entity was recorded in the server database. |
| Change Identifier | Identifies the monitored changes entity for this saved data entity.           |

Saved Data ID is only available to users with the admin role.

## CAS Config domain

Tracks CAS host configurations, where a configuration is the application of one or more template sets to a specific database server host. From configuration instances you can see which items within template sets are enabled or disabled, or exactly which files are selected and monitored (or not) by file name pattern templates. This topic describes the domain's entities and attributes.

Available to roles: all

## Host Entity

---

Identifies a CAS host (a database server) and the current status of CAS (online/offline). A CAS Host entity is created the first time that CAS is seen on a database server host. It is updated each time that the online/offline status changes. The Host entity is available in the CAS Host History domain and the CAS Config domain.

| Attribute | Description                                             |
|-----------|---------------------------------------------------------|
| Host Id   | Host ID                                                 |
| Host Name | Database server host name (might display as IP address) |
| IP        | Host IP                                                 |
| Is Online | Online status (Yes/No) when record was written          |
| OS Type   | Operating system: UNIX or WIN                           |

## Instance Config entity

---

An Instance Config Entity is created each time that an instance configuration is defined. This entity defines how the CAS instance connects to the database (if necessary), and identifies the template set used by the instance.

| Description     | Description                                                                                              |
|-----------------|----------------------------------------------------------------------------------------------------------|
| DB Type         | Database Type (Oracle, MS-SQL, DB2®, Sybase, Informix®, etc.) or N/A for an operating system instance.   |
| Instance        | The name of the instance.                                                                                |
| User            | The user name that CAS uses to log onto the database; or N/A for an operating system instance.           |
| Port            | The port number CAS uses to connect to the database; this can be empty for an operating system instance. |
| DB Home Dir     | The home directory for the database; this can be empty for an operating system instance.                 |
| Template Set ID | Identifies the template set used by this instance.                                                       |

## Datasource entity

---

| Attribute             | Description                                                                                                                         |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Connection Properties | Reported only if additional connection properties are included on the JDBC URL to establish a JDBC connection with this datasource. |
| Data-Source Severity  | Severity Classification (or impact level) if defined for the datasource.                                                            |
| Database Name         | If defined for the datasource: schema name for DB2 or Oracle datasource. Database name for others.                                  |
| Database Description  | Longer description of the datasource, if defined.                                                                                   |
| Database ID           | Database ID                                                                                                                         |
| Database Name         | If defined for the datasource: schema name for DB2 or Oracle datasource. Database name for others.                                  |
| Database Type         | The datasource type.                                                                                                                |
| Host                  | Host name or IP address                                                                                                             |
| Last Connect          |                                                                                                                                     |
| Port                  | Port, if defined for the datasource                                                                                                 |
| Service Name          | For a DB2 datasource, the database name. For Oracle, Informix, and IBM ISeries, the service name.                                   |
| Shared                | True/false. True indicates that this datasource is shared with other applications.                                                  |
| User Name             | User name, if defined for this datasource.                                                                                          |

## CAS Host History domain

---

Tracks CAS host events, including servers or clients going in or out of service. This topic describes the domain's entities and attributes.

Available to roles: all

## Host Entity

---

Identifies a CAS host (a database server) and the current status of CAS (online/offline). A CAS Host entity is created the first time that CAS is seen on a database server host. It is updated each time that the online/offline status changes. The Host entity is available in the CAS Host History domain and the CAS Config domain.

| Attribute | Description                                             |
|-----------|---------------------------------------------------------|
| Host Id   | Host ID                                                 |
| Host Name | Database server host name (might display as IP address) |
| IP        | Host IP                                                 |
| Is Online | Online status (Yes/No) when record was written          |
| OS Type   | Operating system: UNIX or WIN                           |

## Host Event Entity

---

Date and time of an event in the CAS client/server relationship. A host event entity is created each time an event is detected or signaled (see the event types) by CAS.

| Attribute           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Audit Host Event Id | Identifies the host event entity                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Audit Host Id       | Identifies the host                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Event Time          | Date and time that the event was recorded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Event Type          | Identifies the event being recorded:<br>Client Up - CAS started on database server host<br><br>Client Down - CAS stopped on database server host<br><br>Failover Off - A server is available (following a disruption), so CAS data is being written to the server<br><br>Failover On - The server is not available, so CAS data is being written to the failover file<br><br>Server Down - The database server stopped<br><br>Server Up - The database server started                                                                                                                                        |
| Original Timezone   | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br><br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00. This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |
| Timestamp           | Timestamp for creation of the entity                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## CAS Templates domain

Track CAS template definitions. Templates identify items to be monitored for changes. Monitored items can be files, environment or registry variables, OS or SQL script output sets, or the set of logged on users. This topic describes the domain's entities and attributes.

Available to roles: all

### Template Set entity

Describes a template set definition. A Template Set entity is created for each template set, which is a set of template items for a particular operating system or database.

| Attribute         | Description                                                                                                                                                                                                                                                                           |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Template Set ID   | A unique identifier for the template set, numbered sequentially                                                                                                                                                                                                                       |
| OS Type           | Operating system: Unix or Windows                                                                                                                                                                                                                                                     |
| DB Type           | Database Type (Oracle, MS-SQL, DB2®, Sybase, Informix®, etc.) or N/A for an operating system template                                                                                                                                                                                 |
| Template Set Name | The template name                                                                                                                                                                                                                                                                     |
| IsDefault         | Indicates whether or not this template is the default for the specified OS type and DB type combination                                                                                                                                                                               |
| Editable          | Indicates whether or not this template can be modified. The default Guardium® templates cannot be modified. In addition, once a template set has been used in a CAS instance, it cannot be modified. However, a template set can always be cloned and the cloned set can be modified. |
| Timestamp         | Date and time the template was last updated                                                                                                                                                                                                                                           |

### Template entity

Describes a template item within a template set.

| Attribute                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Template ID               | A unique identifier for the template set, numbered sequentially                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Access Name               | Depending on the Audit Type, this is the OS or SQL script, environment or registry value, or a file name or a file name pattern                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Audit Type                | The type of monitored item                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Audit Frequency (minutes) | The maximum interval (in minutes) between tests                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Use MD5                   | Indicates whether or not the comparison is done by calculating a checksum using the MD5 algorithm and comparing that value with the value calculated the last time the item was checked. The default is to not use MD5. If MD5 is used but the size of the raw data is greater than the MD5 Size Limit configured for the CAS host, the MD5 calculation and comparison will be skipped. Regardless of whether or not MD5 is used, both the current value of the last modified timestamp for the item and the size of the item are compared with the values saved the last time the item was checked. |
| Save Data                 | Indicates if the Keep Data checkbox has been marked. If so, previous versions of the item can be compared with the current version.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Description               | Optional description of the template                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Timestamp                 | Date and time the template was last updated.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Catalog domain: entities and attributes

The Guardium catalog tracks where every archive or backup is sent. The catalog domain presents catalog details.

### Entry entity

| Attribute                 | Description                                                                                                                                               |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Aggregator                | Aggregator from which archive or backup was created.                                                                                                      |
| Audit Process Description | Description of the audit process that was archived/backed up.                                                                                             |
| Comment                   | User added comment.                                                                                                                                       |
| Disk Space                |                                                                                                                                                           |
| From Date                 | Start date of the data that is archived.                                                                                                                  |
| Global ID                 | Unique ID.                                                                                                                                                |
| Guardium version          | Version of managed unit.                                                                                                                                  |
| Run Number                | Audit process results run number.                                                                                                                         |
| Step                      | Entry can archived and purged, or archived not purged. If the archive has a catalog entry location, then also where it's archived stored the credentials. |
| Timestamp                 | Last time table was updated.                                                                                                                              |
| To Date                   | End date of the data that is archived.                                                                                                                    |
| Type                      | Data or audit process result can also be a system backup.                                                                                                 |

## Location Entity

How to determine what days are not archived

catalog entry

Use a query (Tools tab > Report Building > Report Builder > query Location View) that can be modified to create a report showing the files that are archived. This report lists all the files with archive dates. Dates not on this report indicate that those dates have not been archived. Run archive for the dates not on the list, if required.

| Attribute | Description                               |
|-----------|-------------------------------------------|
| Host      | Host name where backup/archive is stored. |
| Path      | Path to backup/archive files.             |
| Retention |                                           |
| User Name | User that has access to this location.    |

## Used By entity

| Attribute     | Description |
|---------------|-------------|
| Mount Event   |             |
| Mount Time    |             |
| Request Count |             |
| Used By       |             |

## Destination entity

| Attribute   | Description                                                            |
|-------------|------------------------------------------------------------------------|
| Class ID    | The system name. Can also be a storage system, ESM, Amazon, and so on. |
| System Type | related                                                                |

## Classification Process Results domain

Reports on classifier process runs and results. This topic describes the domain's entities and attributes.

Available to roles: all

## Classification Process Run Entity

This entity describes a classification process job execution.

| Attribute           | Description                                                              |
|---------------------|--------------------------------------------------------------------------|
| Process Description | From the process definition.                                             |
| Status              | Job status.                                                              |
| Queue DateTime      | Timestamp when the job was submitted to the classifier/assessment queue. |
| Start DateTime      | Timestamp at start of job.                                               |
| End DateTime        | Timestamp at end of job.                                                 |
| Data Sources        | Timestamp at end of job.                                                 |

## Classification Process Results Entity

This entity is created for each classification process rule that is fired.

| Attribute | Description                       |
|-----------|-----------------------------------|
| Catalog   | Catalog location for results set. |

| Attribute               | Description                                 |
|-------------------------|---------------------------------------------|
| Schema                  | Schema name if applicable.                  |
| Table Name              | Table name from the rule definition.        |
| Column Name             | Column name from the rule definition.       |
| Rule Description        | The classifier policy rule description.     |
| Comments                | Any comments added to this rule definition. |
| Classification Name     | Classification for the rule.                |
| Category                | Category for the rule.                      |
| Data Source Description | Data source for the rule.                   |

## CM Buffer Usage Monitor domain

Shows the aggregate of all Sniffer Buffer Usage Entities that have been uploaded to the central manager. This topic describes the domain's entities and attributes.

### CM Buffer Usage Monitor entity

| Attribute                      | Description                                                                                                 |
|--------------------------------|-------------------------------------------------------------------------------------------------------------|
| Sniffer Buffer Usage ID        | Unique ID.                                                                                                  |
| Timestamp                      | Time the record was created.                                                                                |
| Sniffer CPU PCT                | Percentage of CPU used by sniffer.                                                                          |
| Sniffer Mem PCT                | Percentage of memory used by sniffer.                                                                       |
| MySQL CPU PCT                  | Percentage of CPU used by MySQL.                                                                            |
| MySQL MEM PCT                  | Percentage of memory used by MySQL.                                                                         |
| PID                            | Sniffer process identifier.                                                                                 |
| Memory                         | Amount of memory used by sniffer.                                                                           |
| Time                           | Elapsed time used by sniffer.                                                                               |
| Free Buffer                    | Amount of free buffer space.                                                                                |
| Analyzer Rate                  | Rate at which messages being analyzed.                                                                      |
| Analyzer Queue                 | Size of the analyze queue.                                                                                  |
| Analyzer Total                 | Total number of messages analyzed.                                                                          |
| Logger Queue                   | Size of logger queue.                                                                                       |
| Logger Total                   | Total number of message logged.                                                                             |
| Session Queue                  | Size of session queue.                                                                                      |
| Session Total                  | Total number of sessions.                                                                                   |
| Handler Data                   | Internal sniffing engine data.                                                                              |
| Extra STR                      | Internal sniffing engine data.                                                                              |
| Sniffer Connections Used       | Total number of connections currently being monitored since inspection engine was restarted.                |
| Sniffer Packets Dropped        | Packets dropped by sniffer.                                                                                 |
| Sniffer Packets Ignored        | Packets ignored by sniffer.                                                                                 |
| Sniffer Packets Throttled      | Total number of connections that have been ignored due to throttling since inspection engine was restarted. |
| Sniffer Connections Ended      | Total number of connections that were monitored and have ended since inspection engine was restarted.       |
| Logger Session Count           | Count of sessions logged.                                                                                   |
| Logger Packets Ignored by Rule | Packets ignored by policy rule action.                                                                      |
| Analyzer Lost Packets          | Packets lost by analyzer.                                                                                   |
| Logger Dbs Monitored           | List of database types currently being monitored.                                                           |
| Mysql Is Up                    | Boolean indicator for internal database restart (1=was restarted, 0=not restarted).                         |
| System Cpu Load                | System CPU utilization.                                                                                     |
| System Uptime                  | Time since last start-up.                                                                                   |
| Mysql Disk Usage               | MySQL disk usage.                                                                                           |
| System Memory Usage            | System memory utilization.                                                                                  |
| System Var Disk Usage          | System var disk utilization.                                                                                |
| System Root Disk Usage         | System Root disk utilization.                                                                               |
| Eth0 Received                  | Messages received on the primary interface.                                                                 |
| Eth0 Sent                      | Messages sent on the primary interface.                                                                     |
| Promiscuous Received           | Rate of received packets through the sniffing network cards (non-interface ports).                          |
| Open FDs                       | Open File Descriptors.                                                                                      |
| Open FDs MySQL                 | Database open File Descriptors                                                                              |
| Sessions normal                | Count of normal sessions.                                                                                   |
| Sessions not opened            | Count of sessions not opened by sniffer.                                                                    |
| Sessions timeout               | Count of sessions timed-out.                                                                                |
| Sessions ignored               | Count of sessions ignored by sniffer.                                                                       |
| Session Direct closed          | Count of sessions directly closed .                                                                         |
| Session guessed                | Count of sessions guessed.                                                                                  |
| SqlGuard Timestamp             | The time that the record is inserted into the custom table                                                  |
| Datasource Name                | Name of the data source used to upload the record                                                           |
| Analyzer Queue Drops           | The number of analyzer queue entries dropped by the sniffer.                                                |

| Attribute            | Description                                                  |
|----------------------|--------------------------------------------------------------|
| Priority Queue Drops | The number of priority queue entries dropped by the sniffer. |

## Comments domain

User defined comments for various Guardium components. This topic describes the domain's entities and attributes.

Available to roles: all

### Comments Entity

This entity describes a user comment. It is available in the Comments domain only, which is restricted to admin users. This domain includes only sharable comments, which are all comments except for those that run locally (see [Local Comments Entity](#)).

| Attribute           | Description                                                                                                                                         |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Comment Creator     | The Guardium® user who created the comment.                                                                                                         |
| Comment Reference   | Indicates the element to which the comment is attached - a query, audit process result, or another comment, for example.                            |
| Content of Comment  | The complete comment text.                                                                                                                          |
| Timestamp           | Date and time the comment was created.                                                                                                              |
| Timestamp Year      | Year only from the timestamp.                                                                                                                       |
| Timestamp WeekDay   | Weekday only from the timestamp.                                                                                                                    |
| Timestamp Time      | Time only from the timestamp.                                                                                                                       |
| Timestamp Date      | Date only from the timestamp.                                                                                                                       |
| Object Description  | The name of the object from which the comment was defined. For example, a comment defined on a policy has an object description of ACCESS_RULE_SET. |
| Record Associations | A list of records that this comment is associated with.                                                                                             |

### Local Comments Entity

This entity describes a local comment. It is available in the Comments domain only, which is restricted to admin users. This entity includes only local comments, for processes and results sets that run locally. Comments that are sharable are defined in the Comments entity.

| Attribute           | Description                                                                                                                                     |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Comment Creator     | The Guardium user who created the comment.                                                                                                      |
| Comment Reference   | Indicates the element to which the comment is attached - a query, audit process result, or another comment, for example.                        |
| Content of Comment  | The complete comment text.                                                                                                                      |
| Timestamp           | Date and time the comment was created.                                                                                                          |
| Timestamp Year      | Year only from the timestamp.                                                                                                                   |
| Timestamp WeekDay   | Weekday only from the timestamp.                                                                                                                |
| Timestamp Time      | Time only from the timestamp.                                                                                                                   |
| Timestamp Date      | Date only from the timestamp.                                                                                                                   |
| Object Description  | The name of the object from which the comment was defined. For example, a comment defined on an incident has an object description of INCIDENT. |
| Record Associations | A list of records that this comment is associated with.                                                                                         |

## Custom DB Usage domain

Custom DB statistics. This topic describes the domain's entities and attributes.

Available to roles: admin

### Custom DB Disk Usage Entity

| Attribute                        | Description                                            |
|----------------------------------|--------------------------------------------------------|
| Number of InnoDB Tables          | Number of InnoDB Tables                                |
| Number of MyISAM Tables          | Number of MyISAM Tables                                |
| Number of Tables                 | Number of Tables                                       |
| Timestamp                        | Timestamp when the data on this row is created/updated |
| Total Size of InnoDB Tables (MB) | Total Size of InnoDB Tables in MB                      |
| Total Size of MyISAM Tables (MB) | Total Size of MyISAM Tables in MB                      |

## Custom Table Disk Usage entity

---

| Attribute         | Description             |
|-------------------|-------------------------|
| Custom Table Name | Custom table name       |
| Table Size (MB)   | Size of the table in MB |
| Table Type        | Table type              |

---

## DB Default Users Enabled domain

Details on whether default users are enabled. This topic describes the domain's entities and attributes.

Available to roles: admin

Non-credential Scan: A process to scan a list of databases and check whether default users are enabled. The default users as well as the list of servers to scan are provided as parameters to the API. A default group is provided for each database type with the default users and passwords created by the database on every installation, customers can add/remove from that list. The groups are of type DB User/DB Password and the names of the default groups are:

ORACLE Default Users; DB2 Default Users; SYBASE Default Users; MS SQL SERVER Default Users; INFORMIX Default Users; MYSQL Default Users; TERADATA Default Users; IBM ISERIES Default Users; POSTGRESQL Default Users; NETEZZA Default Users

## DB Default Users Enabled Entity

---

| Attribute     | Description                  |
|---------------|------------------------------|
| DB Type       | Database type                |
| DB Version    | Database version             |
| Host Name     | Host name of this database   |
| Instance Name | Database instance name       |
| Port          | Port number of this database |
| Timestamp     |                              |
| User Name     | User name                    |

---

## Discovered Instances domain

Instances that have been discovered by GIM. This topic describes the domain's entities and attributes.

Available to roles: all

## Discovered Instances Entity

---

This entity identifies discovered instances.

| Attribute                      | Description                                                                                                           |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Timestamp                      | A timestamp value created when Guardium® records this instance of the entity (every instance has a unique timestamp). |
| Host                           | Host name for this instance                                                                                           |
| Protocol                       | Protocol specific to this instance                                                                                    |
| Port Min                       | Port range, minimum port number for inspection-engines                                                                |
| Port Max                       | Port range, maximum port number for inspection-engines                                                                |
| Client IP                      | IP address/mask of client                                                                                             |
| Exclude Client IP              | IP address/mask of clients to exclude                                                                                 |
| Proc Names                     | Name of database executable                                                                                           |
| Named Pipe                     | Pipe name used by database                                                                                            |
| KTAP DB Port                   | Database port for KTAP                                                                                                |
| DB Install Dir                 | Database Install Directory                                                                                            |
| Proc Name                      | Process name                                                                                                          |
| DB2 Shared Mem Adjustment      | Packet header size                                                                                                    |
| DB2 Shared Mem Client Position | Client I/O area offset                                                                                                |
| DB2 Shared Mem Size            | DB2 shared memory segment size                                                                                        |
| Instance Name                  | Name of the discovered instance                                                                                       |
| Informix Version               | Major version of the database version                                                                                 |
| Unix Socket                    | UNIX socket                                                                                                           |
| DB User                        | The name of the database user                                                                                         |
| DB Version                     | The database version                                                                                                  |

---

## Distributed Datamart domain

Data on distributed data marts. This topic describes the domain's entities and attributes.

## Distributed Datamart status Entity

| Attribute                       | Description                                                                   |
|---------------------------------|-------------------------------------------------------------------------------|
| Datamart ID                     | Distributed Datamart unique ID.                                               |
| Datamart Name                   | Distributed Datamart name.                                                    |
| Details                         | Distributed Datamart execution details.                                       |
| End Time                        | The time when the distributed datamart finished collecting data on this unit. |
| Hostname                        | Host name of unit from which the distributed datamart collected data from.    |
| Query ID                        | ID of the query based on which the distributed datamart is defined.           |
| Report ID                       | ID of the report based on which the distributed datamart is defined.          |
| Report Title                    | Title of the report based on which the distributed datamart is defined.       |
| Run ID                          | Distributed datamart execution unique ID.                                     |
| Send to Secondary Target Status | Status of data consolidation on the second target.                            |
| Start Time                      | The time when the distributed datamart started to collect data on this unit.  |
| Status                          | Status of data collection on the primary target.                              |
| Status Id                       | Distributed datamart status unique ID.                                        |
| Timestamp                       | Timestamp of distributed datamart status change.                              |
| User Id                         | User that owns the distributed datamart.                                      |

## Eagle Eye domain

Data on the Threat Detection Analytics. This topic describes the domain's entities and attributes.

Available to roles: admin.

### Case entity

| Attribute       | Description                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------|
| Seen From       | First recorded symptom for this suspected attack.                                            |
| Case End        | Last recorded symptom for this suspected attack.                                             |
| Case ID         | Unique identifier for the suspected attack.                                                  |
| Case Type Id    | Attack type, for example: SP (malicious STP), SQLI (SQL injection).                          |
| Confidence(%)   | Certainty that this is an attack and not legitimate activity                                 |
| Creation Time   | Time of the first recorded symptom for this suspected attack.                                |
| DB Type         | Type of DB that is the target of the suspected attack.                                       |
| DB User Name    | DB Name that was used to perform the suspicious activity.                                    |
| Risk            | Risk that the suspected attack can compromise sensitive data: 1 (low), 2 (medium), 3 (high). |
| STP Id          | In case of malicious SP, the unique identifier of the stored procedure.                      |
| Server IP       | IP address that is the target of the suspected attack.                                       |
| Service Name    | Service Name that is the target of the suspected attack.                                     |
| Source Program  | Source program that is the target of the suspected attack.                                   |
| TimeStamp       | Creation time of this record.                                                                |
| Additional Info | Additional details about the suspected attack.                                               |

### Case Type entity

Metadata table of threat detection cases.

| Attribute      | Description                              |
|----------------|------------------------------------------|
| Case Type Id   | Attack ID.                               |
| Case Type Name | Attack name.                             |
| Description    | General information about the case type. |
| Timestamp      | Timestamp of this record.                |

### Case Symptom Link entity

Link table.

| Attribute  | Description |
|------------|-------------|
| Case Id    | Case ID.    |
| Symptom Id | Symptom ID. |

### Case Symptom entity

| Attribute | Description |
|-----------|-------------|
|           |             |

| Attribute       | Description                                                             |
|-----------------|-------------------------------------------------------------------------|
| Construct Id    | The related SQL construct ID.                                           |
| Count           | Number of occurrences of this symptom.                                  |
| Description     | Symptom description.                                                    |
| Details         | Additional details.                                                     |
| Error           | The suspected SQL error that generated the symptom.                     |
| Original SQL    | The suspected SQL statement that generated the symptom.                 |
| STP Id          | In case of malicious SP, the unique identifier of the stored procedure. |
| Seen From       | Time this symptom was first recorded.                                   |
| Severity        | Assigned score, used when calculating the risk.                         |
| Symptom End     | Time this symptom was last recorded.                                    |
| Symptom Id      | Unique identifier for this symptom.                                     |
| Symptom Type Id | Unique identifier for this symptom type.                                |
| TimeStamp       | Timestamp of this record.                                               |
| Additional Info |                                                                         |

## Symptom Type entity

Metadata table, except for "Is Active"

| Attribute                  | Description                                     |
|----------------------------|-------------------------------------------------|
| Description                | Text description.                               |
| Is Active                  | Whether or not Guardium scans for this symptom. |
| Symptom Description Prefix | Symptom Description Prefix.                     |
| Symptom Group              | Symptom Group                                   |
| Symptom Name               | Text name of symptom.                           |
| Symptom type Id            | Unique identifier for symptom type.             |
| TimeStamp                  | Timestamp of this record.                       |

## Exceptions domain

This domain contains traffic details: all of the exceptions and exception-related data. These are SQL exceptions sent from a database server and collected by inspection engines, as well as exceptions generated by Guardium itself. This topic describes the domain's entities and attributes.

Available to roles: all

## Client/Server Entity

This entity describes a specific client-server connection. An instance is created each time a unique set of attributes (excluding the Timestamp) is detected.

Note: For Access Tracking only, Client/Server Entity name appears in the menu as two possible entities - Client/Server and Client/Server By Session. Client/Server By Session gets its count from the Client/Server and date conditions from the Session.

Client/Server gets its count from the Client/Server and date conditions also from the Client/Server.

If you select Client/Server, then the query is populated with ATTRIBUTE\_ID = 1. If you select Client/Server By Session, then the query is populated with MAIN\_ATTRIBUTE\_ID = 0.

| Attribute                                    | Description                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access ID                                    | A unique identifier for this unique set of client/server connection attributes. Only available to users with the admin role.                                                                                                                                                                                                                                                    |
| Analyzed Client IP                           | Applies only to encrypted traffic; when set, client IP is set to zeroes.<br>Analyzed Client IP contains the IP for encrypted sessions. For unencrypted sessions Analyzed Client IP will be the same as Client IP.                                                                                                                                                               |
| Client Host Name                             | Client host name.                                                                                                                                                                                                                                                                                                                                                               |
| Client IP                                    | Client IP address. For ASO traffic, CLIENT_IP is not the actual client IP; use the Analyzed Client IP, which is the correct IP. For Oracle ASO encrypted IPv6 traffic (local as well as remote), use the Client Host Name to identify the actual client session, due to limitations. For SSL traffic, Client IP is not the actual client IP and there is no Analyzed Client IP. |
| ClientIP / DBUser                            | Paired attribute value consisting of the client IP address and database user name.                                                                                                                                                                                                                                                                                              |
| Client IP/Src App/DB User/Server IP/Svc Name | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                             |
| Client IP/Src App/User                       | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                             |
| Client MAC                                   | Client hardware address.                                                                                                                                                                                                                                                                                                                                                        |

| Attribute                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Client OS                  | <p>Client operating system.</p> <p>For Teradata, as there is no direct information about client/server OS, instead, the data format type is used; indicating how integer data are stored during db session. This has a close relation to the platform being used and may appear as follows:</p> <p>IBM MAINFRAME // IBM mainframe data format</p> <p>HONEYWELL MAINFRAME // Honeywell mainframe data format</p> <p>AT&amp;T 3B2 // AT&amp;T 3B2 data format.</p> <p>INTEL 8086 // Intel 8086 data format (IBM PC or compatible)</p> <p>VAX // VAX data format</p> <p>AMDAHL // Amdahl data format</p>                                                                                                                                         |
| DB Protocol                | Protocol specific to the database server For example, DRDA (Db2), TNS (Oracle), or TDS (MS SQL Server).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| DB Protocol Version        | Protocol version for the DB Protocol.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| DB User Name               | Database user name: user that connected to the database, either local or remote.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Last Used                  | The timestamp of the last time the data was used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Network Protocol           | Network protocol used (such as TCP or UDP. For K-TAP on Oracle, this displays as either IPC or BEQ)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| OS User                    | OS user as reported by the database client where supported by the database type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Server Description         | Server description (if any). For example, displays cluster name of the Cloudera Data Platform.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Server Host Name           | Server host name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Server IP                  | Server IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Server IP/DB user          | Paired attribute value consisting of Server IP address and database user name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Server IP/Svc Name/DB User | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Server OS                  | <p>Server operating system.</p> <p>For Informix, the OS may appear as follows:</p> <p>IEEEM indicating Unix or JDBCIEEEI indicating WindowsDEC indicating DEC Alpha</p> <p>For Teradata, as there is no direct information about client/server OS, instead, the data format type is used; indicating how integer data are stored during db session. This has a close relation to the platform being used and may appear as follows:</p> <p>IBM MAINFRAME // IBM mainframe data format</p> <p>HONEYWELL MAINFRAME // Honeywell mainframe data format</p> <p>AT&amp;T 3B2 // AT&amp;T 3B2 data format.</p> <p>INTEL 8086 // Intel 8086 data format (IBM PC or compatible)</p> <p>VAX // VAX data format</p> <p>AMDAHL // Amdahl data format</p> |
| Server Type                | The type of database monitored, such as Dd2, Oracle, or Teradata.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Service Name               | Service name for the interaction. In some cases (AIX shared memory connections, for example), the service name is an alias that is used until the actual service is connected. In those cases, once the actual service is connected, a new session is started - so what the user experiences as a single session is logged as two sessions.<br>For Teradata, Service name contains the session logical host id value.                                                                                                                                                                                                                                                                                                                         |
| Source Program             | Source program as reported by the database client where supported by the database type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Client/ Server by session  | Client/Server by session is also a Main Entity. Access this secondary entity by clicking on the Client/Server primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Timestamp                  | The time on the collector when the client <b>first</b> connected to the server. For example, if a client is connecting to the server in the same way many days in a row this timestamp will be the time of the first connection. This may even be before the purge days of the appliance.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Timestamp Date             | Date only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Timestamp Time             | Time only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Timestamp Weekday          | Weekday only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Timestamp Year             | Year only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## Session Entity

This entity is created for each Client/Server database session.

| Attribute       | Description                                                                                                                                                                                                                                    |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access ID       | A unique identifier for this unique set of client/server connection attributes. Only available to users with the admin role.                                                                                                                   |
| Client Port     | Client port number.                                                                                                                                                                                                                            |
| Database Name   | Name of database for the session.<br>For Oracle, Database Name may contain additional and application specific information such as the currently executing module for a session that has been set in the MODULE column of the V\$SESSION view. |
| Duration (secs) | Indicates the length of time between the Session Start and the Session End (in seconds).                                                                                                                                                       |
| Global ID       | Uniquely identifies the session - access. Only available to users with the admin role.                                                                                                                                                         |
| Ignored Since   | Timestamp created when starting to ignore this session.                                                                                                                                                                                        |

| Attribute             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Inactive Flag         | <ul style="list-style-type: none"> <li>-1: Session closed by timeout.</li> <li>0 (default): Open for sessions generated by SQL package.</li> <li>1: Closed (disconnect/ logout received).</li> <li>2: Closed due to timeout on Guardium system. The session is reopened when traffic is regenerated in the session.</li> <li>3: For sessions generated from non-SQL packets.</li> </ul>                                                                                                                                                                                                                  |
| Old Session ID        | Points to the session from which this session was created. Zero if this is the first session of the connection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Original Timezone     | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00, This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |
| Process ID            | The process ID of the client that initiated the connection (not always available).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Server Port           | Server port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Session Encrypted     | Whether the session is encrypted. 0: no; 1: yes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Session End           | The time on the DB server when the session ended. Session End is also a Main Entity. Access this secondary entity by clicking on the Session primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Session End Date      | Date only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session End Time      | Time only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session End Weekday   | Weekday only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Session End Year      | Year only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session ID            | Uniquely identifies the session. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Session Ignored       | A Yes indicates that the session was ignored using the IGNORE SESSION policy action.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Session Start         | The time on the DB server when the session started. Session Start is also a Main Entity. Access this secondary entity by clicking on the Session primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Session Start Date    | Date only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Session Start Time    | Time only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Session Start Weekday | Weekday only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Session Start Year    | Year only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Terminal Id           | Terminal ID of the connection, used internally to resolve session information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Timestamp             | The time on the collector when the session information was most recently updated. Initially, a timestamp created for the first request on a client-server connection where there is not an active session in progress. Later, it is updated when the session is closed, or when it is marked inactive following an extended period of time with no observed activity. When tracking Session information, you are probably more interested in the Session Start and Session End attributes than the Timestamp attribute. If the session is closed it is the same time as the Session End.                 |
| Timestamp Date        | Date only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timestamp Time        | Time only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timestamp Weekday     | Weekday only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Timestamp Year        | Year only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| TTL                   | Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Uid Chain             | For a session reported by Unix S-TAP (K-TAP mode only), or FAM on Windows, this shows the chain of OS users, when users <b>su</b> with a different user name. For more information, see <a href="#">Linux-Unix: UID chains</a> and <a href="#">UID chain for FAM</a> .                                                                                                                                                                                                                                                                                                                                   |
| Uid Chain Compressed  | The UID chain excluding the first user and the last user. For more information, see <a href="#">Linux-Unix: UID chains</a> and <a href="#">UID chain for FAM</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Client/Server Session Entity

| Attribute                                                     | Description                                                                                         |
|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Client IP/Src App/DB User/Server IP/Svc. Name/OS User/DB Name | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> . |
| Server IP/Server Port                                         | Server IP/Server Port                                                                               |

## Exception Type Entity

There is a fixed set of exception types, one of which is associated with each exception logged. These are available for reporting only from the owning Exception Entity.

| Attribute | Description |
|-----------|-------------|
|-----------|-------------|

| <b>Attribute</b>      | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Exception Description | <p>A text description of the exception type, from the following list. Most of these should never be seen.</p> <p>A new construct was used</p> <p>Alert Process threw an exception</p> <p>Custom Alerting Processing Exception</p> <p>Database Server returned an error</p> <p>For this message, a database error code will be stored in the Exception Description attribute of the Exception entity, and a text version of the database error message will be available in the Database Error Text attribute of the Database Error Text entity.</p> <p>DB Protocol Exception</p> <p>Debug prints through the EXCEPTIONs mechanism</p> <p>Dropped database requests</p> <p>Session information was dropped due to excess traffic.</p> <p>Error During Configuration Auditing System Process</p> <p>Error During Classification Process</p> <p>Invalid Query Invocation</p> <p>Login Failed</p> <p>Low-level DB protocol Exception</p> <p>QRW_EXCEPTION</p> <p>Scheduled job threw an exception</p> <p>Security Assessment Exception</p> <p>Security Exception</p> <p>For this message, a custom class exception has been raised when breaching code execution is blocked; such as when users use the Java™ API to define their own alerts or assessments.</p> <p>Session closed prematurely</p> <p>SQL Parser Exception</p> <p>S-TAP Connectivity reconnect</p> <p>For this message, the IP address or DNS name of the database server will be available in the Exception Description attribute of the Exception entity</p> <p>S-TAP Connectivity timeout</p> <p>For this message, the IP address or DNS name of the database server will be available in the Exception Description attribute of the Exception entity</p> <p>TCP ERROR</p> <p>For this message, additional information about the error will be included in the Exception Description attribute of the Exception entity</p> <p>Turbine class threw an exception</p> <p>Unable to purge report</p> |

## Exception Entity

This entity is created for each exception encountered.

| <b>Attribute</b>    | <b>Description</b>                   |
|---------------------|--------------------------------------|
| App User Name       | Application user name.               |
| Collector Id        |                                      |
| DB2 i Current User  |                                      |
| DB2 i/z Database    |                                      |
| DB2 i/z Program     |                                      |
| Database Protocol   |                                      |
| Destination Address | Destination IP address.              |
| Destination Port    | Destination port number.             |
| Database Protocol   | Database protocol for the exception. |
| Event Microsec      |                                      |
| Exception Date      | Date only from the timestamp.        |

| Attribute                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Exception Description                        | Description of the exception.<br>For an S-TAP reconnect or timeout exception, this field contains the IP address or DNS name of the database server.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|                                              | For a database exception, this is an error code from the database management system. For most common messages (about 54,000 of them), a longer text description is available in the Database Error Text attribute. That text comes from the internal Guardium® database table of error messages, not from the exception itself.                                                                                                                                                                                                                                                                          |
|                                              | For Db2 z/OS systems, this field returns the Event ID return code if a negative SQL code is not available.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Exception ID                                 | Uniquely identifies the exception. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Exception Time                               | Time only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Exception Timestamp                          | The time on the DB Server (if the exception is from monitored traffic, for example, an SQL exception on the database) or Collector (if the exception is related to the collector for example, a parser error).                                                                                                                                                                                                                                                                                                                                                                                           |
| Exception Type ID                            | Uniquely identifies the exception type. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Exception Weekday                            | Weekday only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Exception Year                               | Year only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Global Id                                    | Global identifier for the exception.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Link to more information about the exception | Optional link that is sometimes available, depending on the exception source.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| New TTL value                                | Reserved for admin role use only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Original Timezone                            | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00. This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |
| SQL string that caused the Exception         | The SQL string that caused the exception.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Source Address                               | Source IP address of the exception.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Source Port                                  | Source port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Timestamp(micro sec)                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| User Name                                    | Database user name. On encrypted traffic, where correlation is required, this value may not be available, but it is always available from the DB User Name attribute in the Client/Server entity.                                                                                                                                                                                                                                                                                                                                                                                                        |

## Database Error Text Entity

The text of each common database error message is stored in a table in the Guardium internal database. It is available for reporting only from the owning Exception Entity for each exception that is a database error. Some types of exceptions, for example S-TAP disconnects or reconnects, do not have a database error text.

| Attribute           | Description                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Database Error Text | A database error code followed by a short text description of the error. The error code is taken from the Exception Description attribute of the Exception entity. Using the error code as a key, the error text is obtained from an internal table on the Guardium appliance, which contains the most common error messages (about 54,000 of them).<br>For example: ORA-00942: table or view does not exist |
| Error Code          | Displays the database error code.                                                                                                                                                                                                                                                                                                                                                                            |

## FAM domain

This domain describes file entitlement (privileges) reports. This topic describes the domain's entities and attributes.

Available to roles: admin, fam.

## FAM File Entity

| Attribute          | Description                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Classification     | Classification from the FAM classification.                                                                                                               |
| Content Type       | Content Type                                                                                                                                              |
| Creation Time      | Creation Time                                                                                                                                             |
| Delete Groups      | Groups that have delete permission on the file.                                                                                                           |
| Delete Users       | Users that have delete permission on the file.                                                                                                            |
| Effective End Time |                                                                                                                                                           |
| Execute Groups     | Groups that have execute permission on the file.                                                                                                          |
| Execute Users      | Users that have execute permission on the file.                                                                                                           |
| File Full Name     | File Full Name                                                                                                                                            |
| File ID            | A unique field added by the sniffer.                                                                                                                      |
| File Id            | Created by the FAM crawler. This is a non-unique combination of server IP and file path. It's used to identify a specific file and to update its details. |

| <b>Attribute</b>      | <b>Description</b>                             |
|-----------------------|------------------------------------------------|
| File Name             | File Name                                      |
| File Server           | File Server                                    |
| Is Removed            | File was deleted from server. True/false.      |
| Is Symbolic           | File is symbolic link. True/false              |
| Modification Time     | Modification Time                              |
| Operating System      | Operating System                               |
| Owner                 | Owner                                          |
| Parent Directory Id   | Parent Directory Id                            |
| Parent Directory Path | Parent Directory Path                          |
| Read Groups           | Groups that have read permission on the file.  |
| Read Users            | Users that have read permission on the file.   |
| Scan Id               | Unique ID of the scan                          |
| Scan Time             | When the file was scanned                      |
| Size                  | Size                                           |
| Source Directory Id   | Source directory unique Id                     |
| Source Directory Path | Source directory unique path                   |
| Timestamp             | Time the file was recorded in Guardium.        |
| Write Groups          | Groups that have write permission on the file. |
| Write Users           | Users that have write permission on the file.  |
| hostName              | File server where file is located.             |
| sg_Id Groups          |                                                |
| sg_Id Users           |                                                |
| su_Id Groups          |                                                |
| su_Id Users           |                                                |

## FAM Classification Entity

| <b>Attribute</b>  | <b>Description</b>                                     |
|-------------------|--------------------------------------------------------|
| Category          | Decision plan name                                     |
| Classification ID | Unique classification ID                               |
| Entities          | Type of sensitive data.                                |
| File Id           |                                                        |
| Scan Id           |                                                        |
| Timestamp         | Time the file was discovered and recorded in Guardium. |

## FAM groups domain

FAM groups are used in cases where file privileges are given to user groups that are under users domain. This domain has entities for mapping from users to groups. Only local groups are supported. This topic describes the domain's entities and attributes.

## FAM Event Group Entity

| <b>Attribute</b> | <b>Description</b>                                                                                                          |
|------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Event ID         | Event ID if set from the API. These attributes appear only when the main entity for the query permits this level of detail. |
| Timestamp        | Timestamp of the event                                                                                                      |
| dc_group ID      |                                                                                                                             |
| groupMember ID   |                                                                                                                             |

## FAM Group Member Entity

| <b>Attribute</b>  | <b>Description</b> |
|-------------------|--------------------|
| GroupMember ID    |                    |
| Timestamp         |                    |
| effectiveEndTime  |                    |
| extractionTime    |                    |
| extractorHost     |                    |
| groupMemberId     |                    |
| isLocal           |                    |
| isRemoved         |                    |
| isUser            |                    |
| memberDomain      |                    |
| memberName        |                    |
| parentGroupDomain |                    |
| parentGroupName   |                    |

## FAM Domain Controlled Group Entity

| Attribute                | Description |
|--------------------------|-------------|
| DomainControlledGroup ID |             |
| Timestamp                |             |
| domain                   |             |
| groupId                  |             |
| groupName                |             |
| lastModified             |             |

## FAM System domain

The FAM system domain describes FAM configurations. This topic describes the domain's entities and attributes.

### FAM Status Entity

| Attribute                     | Description                                                                                                              |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Classification Decision Plans | The Classification categories and rules. For example: HIPAA{HIPAA_match,CreditCard,Name};PCI{PCI_match}                  |
| Classification Thread Count   | System parameter for ICM                                                                                                 |
| Crawler Max Depth             | The Discovery and Classification Directory depth of scanning.                                                            |
| Excluded Directories Paths    | The list of directories to exclude from the Discovery and Classification process.                                        |
| Excluded Files Paths          | The list of files to exclude from the Discovery and Classification process.                                              |
| Files Crawler Host            | The file server host name.                                                                                               |
| Files Crawler IP              | The file server ip.                                                                                                      |
| ICM URL                       | System parameter. Classification runs on local server. Usually: http://localhost:18087                                   |
| Is Content Discovery Active   | True - Enable classification on files based on their content.<br>False – Metadata and access permission extraction only. |
| Is Crawler Active             | 0: FAM Discovery agent is disabled.<br>1: FAM Discovery agent is enabled.<br>2: FAM Discovery agent is restarted.        |
| Scheduler Hour Interval       | Interval between scans in hours.                                                                                         |
| Scheduler Is Repeat           | True: scan repeats<br>False: scan does not repeat.                                                                       |
| Scheduler Minute Interval     | Interval between scans in minutes.                                                                                       |
| Scheduler Start Time          | Activation time for scanning.                                                                                            |
| Server IP                     | The Guardium server IP                                                                                                   |
| Source Directories Paths      | Directory paths on which to run scan. For example: /home/ab                                                              |
| Status ID                     | Internal ID                                                                                                              |
| Timestamp                     | Time the scan started.                                                                                                   |

## File Activity Monitor domain

This domain contains file entitlement and classification entities. This topic describes the domain's entities and attributes.

### Scan Entity

| Attribute             | Description                             |
|-----------------------|-----------------------------------------|
| Host IP               | Fileserver host IP.                     |
| Host Name             | Fileserver host name.                   |
| OS                    | Operating system.                       |
| Scan Time             | The scan start time.                    |
| Source Directory ID   | Source directory ID.                    |
| Source Directory Path | Source directory path.                  |
| Timestamp             | Time the data was uploaded to Guardium. |

### Directory entity

| Attribute      | Description                                                   |
|----------------|---------------------------------------------------------------|
| Creation Time  | Directory creation time.                                      |
| Delete Groups  | List of groups that have Delete permission on this directory. |
| Delete Users   | List of users that have Delete permission on this directory   |
| Directory      | Not in use.                                                   |
| Directory ID   | Directory ID                                                  |
| Directory Name | Directory name                                                |
| Directory Path | Directory path                                                |

| Attribute                | Description                                                            |
|--------------------------|------------------------------------------------------------------------|
| Display Size             | The directory Size on the UI.                                          |
| Effective End Time       | Internal parameter                                                     |
| Execute Groups           | List of groups that have Execute permission on this directory          |
| Item Permissions         | Not in use.                                                            |
| Item Type                | Not in use.                                                            |
| Modification Time        | The directory modification time.                                       |
| Owner                    | The directory owner.                                                   |
| Parent Directory ID      | Parent directory ID.                                                   |
| Read Groups              | List of groups that have Read permission on this directory.            |
| Read Users               | List of groups that have Execute permission on this directory.         |
| Scan Time                | The time that the scan started on this directory.                      |
| Size                     | Directory size.                                                        |
| Timestamp                | The time of uploading the directory details to the Guardium appliance. |
| Write Groups Write Users | List of users and groups that have Write permission on this Directory  |
| is Removed               | Whether or not this directory was deleted from the last scan.          |

## File Entity

---

| Attribute          | Description                                                       |
|--------------------|-------------------------------------------------------------------|
| Classification     | The Classification category and entities found.                   |
| Content type       | The file content type.                                            |
| creation Time      | The file creation time.                                           |
| Delete Groups      | List of groups that have Delete permission on this Directory.     |
| Delete Users       | List of users that have Delete permission on this Directory.      |
| Directory ID       | Directory ID.                                                     |
| Directory Path     | The file directory Path.                                          |
| Display Size       | The directory size on the UI.                                     |
| Effective End Time | Internal parameters                                               |
| Execute Groups     | List of groups that have Execute permission on this directory.    |
| Execute Users      | List of users that have Execute permission on this directory.     |
| FAM File Id        | File ID.                                                          |
| File Full Name     | File full name (full path and filename)                           |
| File Id            | File ID.                                                          |
| File Name          | File name.                                                        |
| Is Removed         | Was this file deleted in from last scan?                          |
| Is Symbolic        | Whether or not this is a symbolic link.                           |
| Item Permissions   | Not in use.                                                       |
| Item Type          | Not in use.                                                       |
| Modification Time  | The file modification time.                                       |
| Owner              | The file owner                                                    |
| Read Groups        | List of groups that have Read permission on this directory.       |
| Read Users         | List of users that have Read permission on this directory.        |
| Scan Time          | Time the file was scanned.                                        |
| Size               | File size.                                                        |
| Timestamp          | Time of the file details were uploaded to the Guardium appliance. |
| Write Groups       | List of groups that have Write permission on this directory.      |
| Write Users        | List of users that have Write permission on this directory.       |

## Classification Entity

---

| Attribute | Description                                                   |
|-----------|---------------------------------------------------------------|
| Category  | The Classification category                                   |
| Entities  | The rules of the classification category                      |
| File Id   | The file ID                                                   |
| Timestamp | The time the classification was added to the Guardium system. |

## Flat Log domain

---

Flat log processing activity. This topic describes the domain's entities and attributes.

Available to roles: all

## Client/Server Entity

---

This entity describes a specific client-server connection. An instance is created each time a unique set of attributes (excluding the Timestamp) is detected.

Note: For Access Tracking only, Client/Server Entity name appears in the menu as two possible entities - Client/Server and Client/Server By Session. Client/Server By Session gets its count from the Client/Server and date conditions from the Session.

Client/Server gets its count from the Client/Server and date conditions also from the Client/Server.

If you select Client/Server, then the query is populated with ATTRIBUTE\_ID = 1. If you select Client/Server By Session, then the query is populated with MAIN\_ATTRIBUTE\_ID = 0.

| Attribute                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access ID                                    | A unique identifier for this unique set of client/server connection attributes. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Analyzed Client IP                           | Applies only to encrypted traffic; when set, client IP is set to zeroes.<br>Analyzed Client IP contains the IP for encrypted sessions. For unencrypted sessions Analyzed Client IP will be the same as Client IP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Client Host Name                             | Client host name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Client IP                                    | Client IP address. For ASO traffic, CLIENT_IP is not the actual client IP; use the Analyzed Client IP, which is the correct IP. For Oracle ASO encrypted IPv6 traffic (local as well as remote), use the Client Host Name to identify the actual client session, due to limitations. For SSL traffic, Client IP is not the actual client IP and there is no Analyzed Client IP.                                                                                                                                                                                                                                                                                                                                            |
| ClientIP / DBUser                            | Paired attribute value consisting of the client IP address and database user name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Client IP/Src App/DB User/Server IP/Svc Name | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Client IP/Src App/User                       | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Client MAC                                   | Client hardware address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Client OS                                    | Client operating system.<br>For Teradata, as there is no direct information about client/server OS, instead, the data format type is used; indicating how integer data are stored during db session. This has a close relation to the platform being used and may appear as follows:<br><br>IBM MAINFRAME // IBM mainframe data format<br><br>HONEYWELL MAINFRAME // Honeywell mainframe data format<br><br>AT&T 3B2 // AT&T 3B2 data format.<br><br>INTEL 8086 // Intel 8086 data format (IBM PC or compatible)<br><br>VAX // VAX data format<br><br>AMDAHL // Amdahl data format                                                                                                                                         |
| DB Protocol                                  | Protocol specific to the database server For example, DRDA (Db2), TNS (Oracle), or TDS (MS SQL Server).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| DB Protocol Version                          | Protocol version for the DB Protocol.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| DB User Name                                 | Database user name: user that connected to the database, either local or remote.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Last Used                                    | The timestamp of the last time the data was used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Network Protocol                             | Network protocol used (such as TCP or UDP. For K-TAP on Oracle, this displays as either IPC or BEQ)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| OS User                                      | OS user as reported by the database client where supported by the database type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Server Description                           | Server description (if any). For example, displays cluster name of the Cloudera Data Platform.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Server Host Name                             | Server host name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Server IP                                    | Server IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Server IP/DB user                            | Paired attribute value consisting of Server IP address and database user name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Server IP/Svc Name/DB User                   | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Server OS                                    | Server operating system.<br>For Informix, the OS may appear as follows:<br><br>IEEEM indicating Unix or JDBCIEEEI indicating WindowsDEC indicating DEC Alpha<br><br>For Teradata, as there is no direct information about client/server OS, instead, the data format type is used; indicating how integer data are stored during db session. This has a close relation to the platform being used and may appear as follows:<br><br>IBM MAINFRAME // IBM mainframe data format<br><br>HONEYWELL MAINFRAME // Honeywell mainframe data format<br><br>AT&T 3B2 // AT&T 3B2 data format.<br><br>INTEL 8086 // Intel 8086 data format (IBM PC or compatible)<br><br>VAX // VAX data format<br><br>AMDAHL // Amdahl data format |
| Server Type                                  | The type of database monitored, such as Dd2, Oracle, or Teradata.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Service Name                                 | Service name for the interaction. In some cases (AIX shared memory connections, for example), the service name is an alias that is used until the actual service is connected. In those cases, once the actual service is connected, a new session is started - so what the user experiences as a single session is logged as two sessions.<br>For Teradata, Service name contains the session logical host id value.                                                                                                                                                                                                                                                                                                      |
| Source Program                               | Source program as reported by the database client where supported by the database type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Client/ Server by session                    | Client/Server by session is also a Main Entity. Access this secondary entity by clicking on the Client/Server primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Attribute         | Description                                                                                                                                                                                                                                                                               |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Timestamp         | The time on the collector when the client <b>first</b> connected to the server. For example, if a client is connecting to the server in the same way many days in a row this timestamp will be the time of the first connection. This may even be before the purge days of the appliance. |
| Timestamp Date    | Date only from the timestamp.                                                                                                                                                                                                                                                             |
| Timestamp Time    | Time only from the timestamp.                                                                                                                                                                                                                                                             |
| Timestamp Weekday | Weekday only from the timestamp.                                                                                                                                                                                                                                                          |
| Timestamp Year    | Year only from the timestamp.                                                                                                                                                                                                                                                             |

## Session Entity

This entity is created for each Client/Server database session.

| Attribute             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access ID             | A unique identifier for this unique set of client/server connection attributes. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Client Port           | Client port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Database Name         | Name of database for the session.<br>For Oracle, Database Name may contain additional and application specific information such as the currently executing module for a session that has been set in the MODULE column of the V\$SESSION view.                                                                                                                                                                                                                                                                                                                                                           |
| Duration (secs)       | Indicates the length of time between the Session Start and the Session End (in seconds).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Global ID             | Uniquely identifies the session - access. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Ignored Since         | Timestamp created when starting to ignore this session.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Inactive Flag         | <ul style="list-style-type: none"> <li>• -1: Session closed by timeout.</li> <li>• 0 (default): Open for sessions generated by SQL package.</li> <li>• 1: Closed (disconnect/ logout received).</li> <li>• 2: Closed due to timeout on Guardium system. The session is reopened when traffic is regenerated in the session.</li> <li>• 3: For sessions generated from non-SQL packets.</li> </ul>                                                                                                                                                                                                        |
| Old Session ID        | Points to the session from which this session was created. Zero if this is the first session of the connection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Original Timezone     | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00. This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |
| Process ID            | The process ID of the client that initiated the connection (not always available).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Server Port           | Server port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Session Encrypted     | Whether the session is encrypted. 0: no; 1: yes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Session End           | The time on the DB server when the session ended. Session End is also a Main Entity. Access this secondary entity by clicking on the Session primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Session End Date      | Date only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session End Time      | Time only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session End Weekday   | Weekday only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Session End Year      | Year only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session ID            | Uniquely identifies the session. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Session Ignored       | A Yes indicates that the session was ignored using the IGNORE SESSION policy action.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Session Start         | The time on the DB server when the session started. Session Start is also a Main Entity. Access this secondary entity by clicking on the Session primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Session Start Date    | Date only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Session Start Time    | Time only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Session Start Weekday | Weekday only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Session Start Year    | Year only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Terminal Id           | Terminal ID of the connection, used internally to resolve session information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Timestamp             | The time on the collector when the session information was most recently updated. Initially, a timestamp created for the first request on a client-server connection where there is not an active session in progress. Later, it is updated when the session is closed, or when it is marked inactive following an extended period of time with no observed activity. When tracking Session information, you are probably more interested in the Session Start and Session End attributes than the Timestamp attribute. If the session is closed it is the same time as the Session End.                 |
| Timestamp Date        | Date only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timestamp Time        | Time only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timestamp Weekday     | Weekday only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Timestamp Year        | Year only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| TTL                   | Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Attribute            | Description                                                                                                                                                                                                                                                                  |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Uid Chain            | For a session reported by Unix S-TAP (K-TAP mode only), or FAM on Windows, this shows the chain of OS users, when users <code>su</code> with a different user name. For more information, see <a href="#">Linux-Unix: UID chains</a> and <a href="#">UID chain for FAM</a> . |
| Uid Chain Compressed | The UID chain excluding the first user and the last user. For more information, see <a href="#">Linux-Unix: UID chains</a> and <a href="#">UID chain for FAM</a> .                                                                                                           |

## Flat Log Entity

This entity describes flat log processing activity.

| Attribute             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Full SQL              | The full SQL logged.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Timestamp             | Date and time stamp when logged.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Timestamp Date        | Date portion of the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Timestamp Time        | Time portion of the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Response Time         | Response time for the request in milliseconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Records Affected      | The number of records affected by the request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Succeeded             | Indicates if request was successful (True/False).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Statement Type        | <p>The type of SQL statement</p> <p>SQL: simple, direct SQL command, for example, typed directly into the CLI</p> <p>RAW: PREPARE of a SQL statement for later execution, for example, conn.prepareStatement (select a from b where c=:value)</p> <p>BIND: execution of a prepared statement including bound parameter values</p> <p>Statement type is part of the FULL SQL entity and is audited only if you have configured Log Full Details for this statement within the policy.</p> <p>You can not filter out specific statement types in the policy, for example, audit-only SQL and BIND statements. You can, however, filter these out in reports.</p> |
| Returned Data         | Data returned (if any)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Bind Info             | Bind information for the request                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Bind Variables Values | For DB2/zOS, contains a list of comma separated bind variable                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Original Timezone     | <p>The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.</p> <p>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00. This means that these events occurred 3 hours apart, but at the same respective local time (9 PM).</p>                                            |

## GIM Clients domain

This topic describes the domain's entities and attributes.

Available to roles: admin.

### GIM Clients entity

| Attribute                    | Description                                                               |
|------------------------------|---------------------------------------------------------------------------|
| GIM Client IP                | Client IP address                                                         |
| GIM Client Name              | Client hostname                                                           |
| GIM Client OS                | Client Operating System (for example, Linux)                              |
| GIM Client OS Vendor         | Operating System Vendor (for example, Redhat)                             |
| GIM Client OS Vendor Version | Operating system kernel version (for example, 2.6.32-642.13.1.el6.x86_64) |
| GIM Client State Timestamp   | Time GIM client was created                                               |

### GIM Clients Modules State entity

| Attribute          | Description                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------|
| Connected To       | The appliance this module is connected to.                                                   |
| GIM Module Name    | Module name (for example, 'GIM')                                                             |
| GIM Module State   | Module state (for example, 'INSTALLED', 'FAILED')                                            |
| GIM Module Version | module's Guardium version                                                                    |
| Is Scheduled       | Is module scheduled for an installation/upgrade/uninstall. 0 – not scheduled, 1 - scheduled. |

### GIM Modules Heartbeats entity

| Attribute     | Description                      |
|---------------|----------------------------------|
| GIM Client Id | Client primary key (GIM_CLIENTS) |

| Attribute       | Description                      |
|-----------------|----------------------------------|
| GIM Module Id   | Module primary key (GIM_MODULES) |
| GIM Module Name | Module name                      |
| Last Update     | Last alive time (millisecs)      |
| State           | Modules state (UP/DOWN)          |

## GIM Events domain

Available to roles: all

### GIM Events Entity

This entity describes events that have occurred while using the Guardium Installation Manager (GIM).

| Attribute         | Description                                                                 |
|-------------------|-----------------------------------------------------------------------------|
| Event Generator   | IP address of the client (for example, DB-Server) that generated the event. |
| Event Description | Event Description.                                                          |
| Event Time        | The time when the event occurred.                                           |

## Group domain

Membership in Guardium groups. This topic describes the domain's entities and attributes.

Available to roles: all

### Group Type Entity

This entity describes a type of Guardium group (user, client IP address, command, etc.).

| Attribute  | Description                               |
|------------|-------------------------------------------|
| Group Type | Identifies the group type.                |
| Timestamp  | Date and time the group type was created. |

### Group Entity

This entity describes a group that has been defined to Guardium.

| Attribute         | Description                                 |
|-------------------|---------------------------------------------|
| Group Description | The name of the group.                      |
| Group Subtype     | Subtype, if any, defined for the group.     |
| Timestamp         | Date and time the group entity was created. |

### Group Member Entity

This entity describes a member of a group that has been defined to Guardium.

| Attribute         | Description                                            |
|-------------------|--------------------------------------------------------|
| Group Member      | The name of the group member.                          |
| Timestamp         | Date and time the group member was created or updated. |
| Timestamp Date    | Date only from the timestamp.                          |
| Timestamp Time    | Time only from the timestamp.                          |
| Timestamp Year    | Year only from the timestamp.                          |
| Timestamp Weekday | Weekday only from the timestamp.                       |

## Guard Process Log domain

Logs of processes running on Guardium. This topic describes the domain's entities and attributes.

Available to roles: admin.

### Guard Process Log Entity

| Attribute   | Description                 |
|-------------|-----------------------------|
| Comment     | Comment entered by user.    |
| Log Message | Message logged by Guardium. |

| Attribute    | Description                           |
|--------------|---------------------------------------|
| Process Name | Process name                          |
| Status       | Status                                |
| TIMESTAMP    | Date and time of the comment/message. |

## Guardium Activity domain

All modifications performed by Guardium users to any Guardium entity, such as a report or query definition or modification. This topic describes the domain's entities and attributes.

Available to roles: admin

### Guardium Activity Types

This entity describes the various user activities

| Attribute                 | Description                            |
|---------------------------|----------------------------------------|
| Activity Type Description | Description of the activity            |
| Activity Type ID          | Uniquely identifies the activity type. |

## Guardium User Activity Audit Entity

This entity is created for each Guardium user activity.

| Attribute          | Description                                                     |
|--------------------|-----------------------------------------------------------------|
| Login ID           | ID used for login.                                              |
| User Name          | Guardium® user name for the activity.                           |
| Timestamp          | Created when the activity was logged.                           |
| Modified Entity    | The Guardium entity modified (a group definition, for example). |
| Entity Key Used    | Key used to access the entity.                                  |
| Key Value          | New value of the entity.                                        |
| All Values         | All values altered.                                             |
| Object Description | The name of specific object altered.                            |
| Global ID          | A unique global ID for the session.                             |
| Host Name          | Host name of the user.                                          |

## Guardium Jobs Queue domain

This topic describes the domain's entities and attributes.

Available to roles: admin.

### Guardium jobs queue entity

| Attribute                | Description                             |
|--------------------------|-----------------------------------------|
| End Time                 | Date and time the job completed.        |
| Guardium Job Description | Guardium Job Description                |
| Process Id               | Unique ID                               |
| Process Run Id           | Job run ID                              |
| Process Type             | Process Type                            |
| Queue Time               | Date and time the job entered the queue |
| Report Result ID         |                                         |
| Start Time               | Date and time the job started.          |
| Status                   | Job status                              |
| Task Description         | Scheduled,                              |
| Timestamp                |                                         |
| CLS_LOG_TYPE_DESC        |                                         |
| DETAILS                  |                                         |
| MESSAGE                  |                                         |

## Guardium classification log

| Attribute                | Description |
|--------------------------|-------------|
| Datasources              |             |
| End Time                 |             |
| Guardium JOB Description |             |

| Attribute         | Description |
|-------------------|-------------|
| Process Id        |             |
| Process Run Id    |             |
| Process Type      |             |
| Queue Time        |             |
| Report Result Id  |             |
| Start Time        |             |
| Status            |             |
| Task Description  |             |
| Timestamp         |             |
| CLS_LOG_TYPE_DESC |             |
| Details           |             |
| Message           |             |

## Guardium Login domain

All Guardium user login and logout information. This topic describes the domain's entities and attributes.

Available to roles: admin

### Guardium Users Login Entity

This entity is created each time a user logs in to the Guardium appliance.

| Attribute            | Description                                                                                     |
|----------------------|-------------------------------------------------------------------------------------------------|
| Login ID             | ID used for login.                                                                              |
| User Name            | Created when the Guardium® user logs in or out (there will be one entity per Guardium session). |
| Login Date And Time  | Date and time user logged in.                                                                   |
| Logout Date And Time | Date and time user logged out.                                                                  |
| Login Succeeded      | Indicates if login was successful.                                                              |
| Global Id            | A unique global ID for the session.                                                             |
| Host Name            | Host name of the user.                                                                          |
| Remote Address       | Remote address of the user.                                                                     |

## IMS Event domain

This topic describes the domain's entities and attributes.

Available to roles: all.

### Client/Server Entity

This entity describes a specific client-server connection. An instance is created each time a unique set of attributes (excluding the Timestamp) is detected.

Note: For Access Tracking only, Client/Server Entity name appears in the menu as two possible entities - Client/Server and Client/Server By Session. Client/Server By Session gets its count from the Client/Server and date conditions from the Session.

Client/Server gets its count from the Client/Server and date conditions also from the Client/Server.

If you select Client/Server, then the query is populated with ATTRIBUTE\_ID = 1. If you select Client/Server By Session, then the query is populated with MAIN\_ATTRIBUTE\_ID = 0.

| Attribute                                    | Description                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access ID                                    | A unique identifier for this unique set of client/server connection attributes. Only available to users with the admin role.                                                                                                                                                                                                                                                    |
| Analyzed Client IP                           | Applies only to encrypted traffic; when set, client IP is set to zeroes.<br>Analyzed Client IP contains the IP for encrypted sessions. For unencrypted sessions Analyzed Client IP will be the same as Client IP.                                                                                                                                                               |
| Client Host Name                             | Client host name.                                                                                                                                                                                                                                                                                                                                                               |
| Client IP                                    | Client IP address. For ASO traffic, CLIENT_IP is not the actual client IP; use the Analyzed Client IP, which is the correct IP. For Oracle ASO encrypted IPv6 traffic (local as well as remote), use the Client Host Name to identify the actual client session, due to limitations. For SSL traffic, Client IP is not the actual client IP and there is no Analyzed Client IP. |
| ClientIP / DBUser                            | Paired attribute value consisting of the client IP address and database user name.                                                                                                                                                                                                                                                                                              |
| Client IP/Src App/DB User/Server IP/Svc Name | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                             |
| Client IP/Src App/User                       | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                             |
| Client MAC                                   | Client hardware address.                                                                                                                                                                                                                                                                                                                                                        |

| Attribute                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Client OS                  | <p>Client operating system.</p> <p>For Teradata, as there is no direct information about client/server OS, instead, the data format type is used; indicating how integer data are stored during db session. This has a close relation to the platform being used and may appear as follows:</p> <p>IBM MAINFRAME // IBM mainframe data format</p> <p>HONEYWELL MAINFRAME // Honeywell mainframe data format</p> <p>AT&amp;T 3B2 // AT&amp;T 3B2 data format.</p> <p>INTEL 8086 // Intel 8086 data format (IBM PC or compatible)</p> <p>VAX // VAX data format</p> <p>AMDAHL // Amdahl data format</p>                                                                                                                                         |
| DB Protocol                | Protocol specific to the database server For example, DRDA (Db2), TNS (Oracle), or TDS (MS SQL Server).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| DB Protocol Version        | Protocol version for the DB Protocol.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| DB User Name               | Database user name: user that connected to the database, either local or remote.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Last Used                  | The timestamp of the last time the data was used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Network Protocol           | Network protocol used (such as TCP or UDP. For K-TAP on Oracle, this displays as either IPC or BEQ)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| OS User                    | OS user as reported by the database client where supported by the database type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Server Description         | Server description (if any). For example, displays cluster name of the Cloudera Data Platform.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Server Host Name           | Server host name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Server IP                  | Server IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Server IP/DB user          | Paired attribute value consisting of Server IP address and database user name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Server IP/Svc Name/DB User | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Server OS                  | <p>Server operating system.</p> <p>For Informix, the OS may appear as follows:</p> <p>IEEEM indicating Unix or JDBCIEEEI indicating WindowsDEC indicating DEC Alpha</p> <p>For Teradata, as there is no direct information about client/server OS, instead, the data format type is used; indicating how integer data are stored during db session. This has a close relation to the platform being used and may appear as follows:</p> <p>IBM MAINFRAME // IBM mainframe data format</p> <p>HONEYWELL MAINFRAME // Honeywell mainframe data format</p> <p>AT&amp;T 3B2 // AT&amp;T 3B2 data format.</p> <p>INTEL 8086 // Intel 8086 data format (IBM PC or compatible)</p> <p>VAX // VAX data format</p> <p>AMDAHL // Amdahl data format</p> |
| Server Type                | The type of database monitored, such as Dd2, Oracle, or Teradata.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Service Name               | Service name for the interaction. In some cases (AIX shared memory connections, for example), the service name is an alias that is used until the actual service is connected. In those cases, once the actual service is connected, a new session is started - so what the user experiences as a single session is logged as two sessions.<br>For Teradata, Service name contains the session logical host id value.                                                                                                                                                                                                                                                                                                                         |
| Source Program             | Source program as reported by the database client where supported by the database type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Client/ Server by session  | Client/Server by session is also a Main Entity. Access this secondary entity by clicking on the Client/Server primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Timestamp                  | The time on the collector when the client <b>first</b> connected to the server. For example, if a client is connecting to the server in the same way many days in a row this timestamp will be the time of the first connection. This may even be before the purge days of the appliance.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Timestamp Date             | Date only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Timestamp Time             | Time only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Timestamp Weekday          | Weekday only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Timestamp Year             | Year only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## Session Entity

This entity is created for each Client/Server database session.

| Attribute       | Description                                                                                                                                                                                                                                    |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access ID       | A unique identifier for this unique set of client/server connection attributes. Only available to users with the admin role.                                                                                                                   |
| Client Port     | Client port number.                                                                                                                                                                                                                            |
| Database Name   | Name of database for the session.<br>For Oracle, Database Name may contain additional and application specific information such as the currently executing module for a session that has been set in the MODULE column of the V\$SESSION view. |
| Duration (secs) | Indicates the length of time between the Session Start and the Session End (in seconds).                                                                                                                                                       |
| Global ID       | Uniquely identifies the session - access. Only available to users with the admin role.                                                                                                                                                         |
| Ignored Since   | Timestamp created when starting to ignore this session.                                                                                                                                                                                        |

| Attribute             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Inactive Flag         | <ul style="list-style-type: none"> <li>-1: Session closed by timeout.</li> <li>0 (default): Open for sessions generated by SQL package.</li> <li>1: Closed (disconnect/ logout received).</li> <li>2: Closed due to timeout on Guardium system. The session is reopened when traffic is regenerated in the session.</li> <li>3: For sessions generated from non-SQL packets.</li> </ul>                                                                                                                                                                                                                  |
| Old Session ID        | Points to the session from which this session was created. Zero if this is the first session of the connection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Original Timezone     | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00, This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |
| Process ID            | The process ID of the client that initiated the connection (not always available).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Server Port           | Server port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Session Encrypted     | Whether the session is encrypted. 0: no; 1: yes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Session End           | The time on the DB server when the session ended. Session End is also a Main Entity. Access this secondary entity by clicking on the Session primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Session End Date      | Date only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session End Time      | Time only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session End Weekday   | Weekday only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Session End Year      | Year only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session ID            | Uniquely identifies the session. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Session Ignored       | A Yes indicates that the session was ignored using the IGNORE SESSION policy action.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Session Start         | The time on the DB server when the session started. Session Start is also a Main Entity. Access this secondary entity by clicking on the Session primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Session Start Date    | Date only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Session Start Time    | Time only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Session Start Weekday | Weekday only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Session Start Year    | Year only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Terminal Id           | Terminal ID of the connection, used internally to resolve session information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Timestamp             | The time on the collector when the session information was most recently updated. Initially, a timestamp created for the first request on a client-server connection where there is not an active session in progress. Later, it is updated when the session is closed, or when it is marked inactive following an extended period of time with no observed activity. When tracking Session information, you are probably more interested in the Session Start and Session End attributes than the Timestamp attribute. If the session is closed it is the same time as the Session End.                 |
| Timestamp Date        | Date only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timestamp Time        | Time only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timestamp Weekday     | Weekday only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Timestamp Year        | Year only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| TTL                   | Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Uid Chain             | For a session reported by Unix S-TAP (K-TAP mode only), or FAM on Windows, this shows the chain of OS users, when users <code>su</code> with a different user name. For more information, see <a href="#">Linux-Unix: UID chains</a> and <a href="#">UID chain for FAM</a> .                                                                                                                                                                                                                                                                                                                             |
| Uid Chain Compressed  | The UID chain excluding the first user and the last user. For more information, see <a href="#">Linux-Unix: UID chains</a> and <a href="#">UID chain for FAM</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Access Period Entity

Access Periods are related to Sessions. By default, an access period is one hour long, but this can be changed by the Guardium administrator in the Inspection Engine Configuration (it corresponds to the Logging Granularity).

| Attribute              | Description                                                                                                                                                                                                                                                 |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application Event ID   | The application event ID if set from the API. Appears only when the main entity for the query permits this level of detail. Not available if either Client/Server or Session is the main entity.                                                            |
| Avg Execution Ack Time | Average Execution Acknowledged time in milliseconds                                                                                                                                                                                                         |
| Avg Records Affected   | The average number of records affected. Appears only when the main entity for the query permits this level of detail. Not available if either Client/Server or Session is the main entity.                                                                  |
| Application User       | Can be one of the following attributes: <ul style="list-style-type: none"> <li>The Application User when identified by <a href="#">application user translation</a>.</li> <li>The Application Event Str when identified by the GuardAppUser API.</li> </ul> |

| Attribute                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Average Execution Time        | The average command execution time during the period. This is for SQL statements only. It does not apply to FTP traffic.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Construct ID                  | Uniquely identifies a command construct (for example, select a from b). Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Egress Kbyte count            | Records the number of bytes in responses.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Failed Sqls                   | The number of failed SQL requests. See note at the end of the table. Appears only when the main entity for the query permits this level of detail. Not available if either Client/Server or Session is the main entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Ingress Kbyte count           | Records the number of bytes in requests.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Instance ID                   | Uniquely identifies an instance of a construct. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Original Timezone             | <p>The UTC offset.</p> <p>This is to point out that a UTC offset should be set so that the time from two different collectors that are in two different time zones aggregate correctly. If the offset was not set then there would exist a condition where users would not really be able to determine or see a true representation of when things happened in relation to time.</p> <p>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00, This means that these events occurred 3 hours apart, but at the same respective local time (9 PM).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Period End                    | The time on the collector when the period, as defined by the logging granularity on the appliance (default 1 hour), ended.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Period End Date               | Date only from the period end attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Period End Time               | Time only from the period end attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Period End Weekday            | Weekday only from the period end attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Period Start                  | The time on the collector when the period, as defined by the logging granularity on the appliance (default 1 hour), started.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Period Start Date             | Date only from the period start attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Period Start Time             | Time only from the period start attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Period Start Weekday          | Weekday only from the period start attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Response Length               | The length of the sniffer response for a SQL instance. Not supported for Db2 z/OS systems. For more information, see <a href="#">store log_general_response_length</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Session ID                    | Uniquely identifies a session. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Show Seconds                  | If a the number of accesses per second is being tracked, this contains counts for each second in the access period (usually one hour).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Successful Sqls               | The number of successful SQL requests. See note at the end of the table. Appears only when the main entity for the query permits this level of detail. Not available if either Client/Server or Session is the main entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Timestamp                     | <p>The time on the collector when an SQL construct was executed most recently <i>within a session and within a time period</i>. If the same SQL construct is run 10 times within the same session and time period, it shows the time of the most recent run for all 10 SQLs. This timestamp is the most appropriate to use along with the SQL attribute in reports.</p> <p>Note: Universal Connector traffic may be delayed. In those cases the Timestamp is the time of on the Collector for the most recent update to the SQL construct record for the session within a time period. Period start still reflects the time of SQL execution according to the audit data source, not the time of record update.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Total Access                  | Total count of construct instances for this access period. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Total Records Affected        | The total number of records affected. Appears only when the main entity for the query permits this level of detail. Not available if either Client/Server or Session is the main entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Total Records Affected (Desc) | <p>If the Total Records Affected attribute is a character string instead of a number, that value appears here (for example, Large Results Set, or N/A). Appears only when the main entity for the query permits this level of detail. Not available if either Client/Server or Session is the main entity.</p> <p>Records affected - Result set of the number of records which are affected by each execution of SQL statements.</p> <p>Note: The records affected option is a sniffer operation which requires sniffer to process additional response packets and postpone logging of impacted data which increases the buffer size and might potentially have a adverse effect on overall sniffer performance. Significant impact comes from really large responses. To prevent large amount of overhead associated with this operation, Guardium uses a set of default thresholds that allows sniffer to decide to skip processing operation when exceeded.</p> <p>You can use the <b>store max_results_set_size</b>, <b>store max_result_set_packet_size</b>, and <b>store max_tds_response_packets</b> CLI commands to set levels of granularity.</p> <p>Example of result set values:</p> <ul style="list-style-type: none"> <li>• Case 1, record affected value, positive number. This represents correct size of the result set.</li> <li>• Case 2, record affected value, -2. This means number of records exceeded configurable limit (This can be tuned through CLI commands).</li> <li>• Case 3, record affected value, -1. This shows any unsupported cases of packets configurations by Guardium.</li> <li>• Case 4, record affected value, -2. If the result set is sent by streaming mode.</li> <li>• Case 5, record affected value, less than -2. Intermediate result during record count to update user about current value, ends up with positive number of total records. For example, the server returns 1000 records in 4 packets: <ul style="list-style-type: none"> <li>◦ Packet #1 250</li> <li>◦ Packet #2 200</li> <li>◦ Packet #3 250</li> <li>◦ Packet #4 200</li> </ul> </li> </ul> <p>Then records affected are reported as</p> <ul style="list-style-type: none"> <li>◦ Packet #1 -250</li> <li>◦ Packet #2 -500</li> <li>◦ Packet #3 -750</li> <li>◦ Packet #4 1000</li> </ul> |

## SQL Entity

This entity is created for each unique string of SQL. Values are replaced by question marks - only the format of the string is stored.

| Attribute     | Description                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------|
| Bind Info     | Bind information for this SQL string.                                                                           |
| Construct ID  | Uniquely identifies the construct in which the SQL appeared                                                     |
| Sql           | SQL string.                                                                                                     |
| Truncated SQL | Indicates if the SQL has been truncated or not where:<br>0 - false/no, not truncated<br>1 - true/yes, truncated |

## FULL SQL Entity

Full SQL entities are created only by the following policy rule actions: Log Full Details, Log Full Details With Values, Log Full Details Per Session, or Log Full Details Per Session With Values.

| Attribute               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access Rule Description | Description of the policy rule whose action triggered the logging of the Full SQL record.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Ack Response Time       | Acknowledged Response Time in milliseconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Auto-Commit             | Entries are automatically numbered.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Bind Variables Values   | For DB2/zOS, a list of comma-separated bind variables.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Full Sql                | The logged SQL statement.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Full SQL ID             | Unique identifier for the Full SQL. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Instance ID             | Unique identifier for the Full SQL instance. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Original Timezone       | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br><br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00. This means that these events occurred 3 hours apart, but at the same respective local time (9 PM).                         |
| Records Affected        | The number of records affected for each session. On reports using this attribute, we suggest that you turn on aliases to properly display special cases such as Large Result Set or N/A.<br>Records affected only supports find statements for MongoDB, and does not support insert, update, and delete statements.                                                                                                                                                                                                                                                                                                                  |
| Records Affected (Desc) | When the Records Affected is a string value instead of a number, that string is stored here. For example: Large Result Set or N/A.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Response Length         | The length of the sniffer response for a SQL instance. Not supported for Db2 z/OS systems. For more information, see <a href="#">store log_general_response_length</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Response Time           | The response time for the request in milliseconds. When requests are monitored in network traffic, the response times are an accurate reflection of the time taken to respond to the request (Guardium timestamps both the client request and the server response).                                                                                                                                                                                                                                                                                                                                                                  |
| Returned Data           | Data returned for this request (if any, and if available).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Returned Data Count     | Number of rows returned from the SQL statement used in the policy rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Statement Type          | The type of SQL statement.<br>SQL: simple, direct SQL command, for example, typed directly into the CLI<br>RAW: PREPARE of a SQL statement for later execution, for example, conn.prepareStatement (select a from b where c=:value)<br>BIND: execution of a prepared statement including bound parameter values<br>Statement type is part of the FULL SQL entity and is only audited if you have configured Log Full Details for this statement within the policy.<br>You can not filter out specific statement types in the policy, for example, audit-only SQL and BIND statements. You can, however, filter these out in reports. |
| Succeeded               | Indicates if the call succeeded. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Timestamp               | The time when the SQL started running in the database server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## FULL SQL Values Entity

These entities are created only by the following policy rule actions: Log Full Details With Values, and Log Full Details Per Session With Values.

| Attribute | Description                                                                                                                              |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------|
| Values    | One or more values from the logged construct.                                                                                            |
| Timestamp | The time on the DB server that the SQL was executed. Traffic must be captured with log full details policy action to see this timestamp. |

## IMS application event link entity

| Attribute                            | Description                                    |
|--------------------------------------|------------------------------------------------|
| IMS Application Event Link ID        | Application Event Id.                          |
| IMS Correlation IMSID:Correlation ID | IMS Correlation IMSID field from S-TAP message |

## IMS application event entity

| Attribute               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application Event ID    | Unique identifier for this application events entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Event Date              | Datetime value, set by GuardAppEvent:Start. It displays in the format yyyy-mm-dd hh:mm:ss.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Event Release Date      | Datetime value, set by GuardAppEvent:Released. It displays in the format yyyy-mm-dd hh:mm:ss.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Event Release Type      | Type of event, set by GuardAppEvent: Released.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Event Release User Name | User name, set by GuardAppEvent: Released.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Event Release Value Num | Numeric value, set by GuardAppEvent: Released.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Event Release Value Str | String value, set by GuardAppEvent: Released.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Event Type              | Type of event, set by GuardAppEvent:Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Event User Name         | User name, set by GuardAppEvent:Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Event Value Num         | Numeric value, set by GuardAppEvent:Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Event Value Str         | String value, set by GuardAppEvent:Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Original Timezone       | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00. This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |
| Timestamp               | Created only once, when the event is logged. Do not confuse this attribute with the Event Date attribute, which can be set using an API call or from a stored procedure parameter. (See a description of the Application Events API in <a href="#">Identify Users with API</a> .)                                                                                                                                                                                                                                                                                                                        |

## Command Entity

For each command, an entity is created for each parent node and position in which the command appears in a command construct.

| Attribute    | Description                                                                                             |
|--------------|---------------------------------------------------------------------------------------------------------|
| Command Id   | Uniquely identifies the command. Only available to users with the admin role.                           |
| Construct Id | Uniquely identifies the construct (e.g., select a from b). Only available to users with the admin role. |
| Depth        | Depth of the command in the SQL parse tree.                                                             |
| Parent       | Identifier of parent node in the parse tree.                                                            |
| SQL Verb     | Main verb in SQL command (e.g., select, insert, delete, etc.).                                          |

## Object Entity

An instance of this entity is created for each object in a unique schema.

| Attribute          | Description                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------|
| App Object Module1 | Uniquely identifies the application object module.                                                                |
| Construct Id       | Uniquely identifies the construct in which the object is referenced. Only available to users with the admin role. |
| Object Id          | Uniquely identifies the object. Only available to users with the admin role.                                      |
| Object Name        | Name of the object.                                                                                               |
| Schema             | Database schema for the object.<br>Note: This attribute is deprecated since it is never populated                 |

## Field Entity

Each time Guardium encounters a new field, it creates a field entity.

| Attribute    | Description                                                                                                                      |
|--------------|----------------------------------------------------------------------------------------------------------------------------------|
| Command ID   | Uniquely identifies the main command from the construct in which it was referenced. Only available to users with the admin role. |
| Construct ID | Uniquely identifies the construct in which it was referenced. Only available to users with the admin role.                       |
| Field ID     | Uniquely identifies the field. Only available to users with the admin role.                                                      |
| Field Name   | Name of the field.                                                                                                               |

| Attribute       | Description                                                                                                                |
|-----------------|----------------------------------------------------------------------------------------------------------------------------|
| List Clause     | Use these attributes to order complex SQL queries.                                                                         |
| Where Clause    | Example of SQL queries:                                                                                                    |
| Order by Clause | Order by                                                                                                                   |
| Having Clause   | SELECT * FROM dept_costs                                                                                                   |
| Group By Clause | WHERE dept_total >                                                                                                         |
| On Clause       | (SELECT avg FROM avg_cost)<br>ORDER BY department                                                                          |
|                 | Having                                                                                                                     |
|                 | SELECT column_name1, SUM(column_name2)                                                                                     |
|                 | FROM table_name                                                                                                            |
|                 | GROUP BY column_name1                                                                                                      |
|                 | HAVING (numerical function condition)                                                                                      |
|                 | Group By                                                                                                                   |
|                 | SELECT column_name1, SUM(column_name2)                                                                                     |
|                 | FROM table_name                                                                                                            |
|                 | GROUP BY column_name1                                                                                                      |
|                 | Where                                                                                                                      |
|                 | SELECT FirstName, LastName, City                                                                                           |
|                 | FROM Users                                                                                                                 |
|                 | WHERE City = Los Angeles                                                                                                   |
| Object ID       | Uniquely identifies the object from the construct in which it was referenced. Only available to users with the admin role. |

## Field SQL Value Entity

These entities are created only by policy rule actions that log with values, for example: Log Full Details With Values, and Log Full Details Per Session With Values. The field value logged may or may not be associated with a field name. For example, field names are available (in the Field entity) if the following statement is logged:

```
insert into t1 (foo, bar) (10, 20)
```

But not available when the following statement is logged:

```
insert into t2 (10, 20)
```

| Attribute | Description                              |
|-----------|------------------------------------------|
| Value     | A field value from the logged construct. |

## Installed Patches domain

Reports on installed patches. This topic describes the domain's entities and attributes.

Available to roles: all.

This domain is available in Guardium systems that have a defined datasource of type GBDI.

## Available Patch Entity

| Attribute          | Description                                                                           |
|--------------------|---------------------------------------------------------------------------------------|
| Creation Date      | The patch creation date.                                                              |
| Guardium Version   | Guardium software version                                                             |
| Patch Dependencies | Guardium version or patch, which has to be installed before this patch.               |
| Patch Description  | Patch Description                                                                     |
| Patch Number       | Patch Number                                                                          |
| Upload Date        | The date the patch was uploaded for installation                                      |
| UTC Offset         | The difference in time between UTC time and time of collector that reported that data |

## Installed Patch Entity

| Attribute | Description |
|-----------|-------------|
|           |             |

| Attribute              | Description                                                             |
|------------------------|-------------------------------------------------------------------------|
| Additional information |                                                                         |
| Creation Date          | The patch creation date.                                                |
| Guardium Version       | Guardium software version                                               |
| Installed By           | CM, SA, or CLI                                                          |
| Patch Dependencies     | Guardium version or patch, which has to be installed before this patch. |
| Patch Description      | Patch Description                                                       |
| Patch Number           | Patch Number                                                            |
| Requested Received     | The date/time the patch should be installed                             |
| Requested Schedule     |                                                                         |
| Status                 | 0/1 for success or failure                                              |
| Status Description     | Patch                                                                   |
| Timestamp              | Timestamp the status was updated.                                       |

## Installed Policy domain

Description of policy parameters and rules for the installed policy. The Installed Policy domain supports multiple policies and multiple actions per rule. This topic describes the domain's entities and attributes.

Available to roles: all

### Installed Policy entity

Describes the installed policy.

| Attribute             | Description                                                           |
|-----------------------|-----------------------------------------------------------------------|
| Audit Pattern         | Test pattern used for a selective audit trail policy.                 |
| ID                    | Identifies the policy installation record.                            |
| Policy Description    | Description from the policy definition.                               |
| Rule Set Id           | Identifies the set of rules.                                          |
| Selective Audit Trail | Indicates if this is a selective audit trail policy (T/F).            |
| Sequence              | Sets the order of sequence when there is multiple installed policies. |
| Timestamp             | Timestamp for the creation of the record.                             |

### Installed Rule entity

| Attribute                                                          | Description                                                                              |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| ACCESS_RULE_ID                                                     | Identifies an access rule.                                                               |
| App Event Date Value                                               | From the rule definition.                                                                |
| App Event Exists                                                   | From the rule definition.                                                                |
| App Event Numeric Value                                            |                                                                                          |
| App Event Text / Numeric / Date                                    | The application event's text, numeric, and date attributes.                              |
| App Event Text Value                                               | From the rule definition.                                                                |
| App User                                                           | From the rule definition.                                                                |
| App User / Group                                                   | A single attribute and a related attribute (if any) in a single column of the report.    |
| App User Group                                                     | From the rule definition.                                                                |
| Category / Classification                                          | The combined category and classification for the rule.                                   |
| Category Name                                                      | From the rule definition.                                                                |
| Classification Name                                                | From the rule definition.                                                                |
| Client IP                                                          | From the rule definition.                                                                |
| Client IP / Group                                                  | A single attribute and a related attribute (if any) in a single column of the report.    |
| Client IP Group                                                    | From the rule definition.                                                                |
| Client IP/Src App/DB User/Server IP/Svc Name Group                 |                                                                                          |
| Client IP/Src App/DB User/Server IP/Svc Name/OS User/DB Name Group |                                                                                          |
| Client MAC                                                         | From the rule definition.                                                                |
| Client Net Mask                                                    | From the rule definition.                                                                |
| Command                                                            | From the rule definition.                                                                |
| Command / Group                                                    | A single attribute and a related attribute (if exists) in a single column of the report. |
| Command Group                                                      | From the rule definition.                                                                |
| Continue to next Rule / Revoke                                     | From the rule definition.                                                                |
| DB Name                                                            | From the rule definition.                                                                |
| DB Name / Group                                                    | A single attribute and a related attribute (if exists) in a single column of the report. |
| DB Name Group                                                      | From the rule definition.                                                                |
| DB Type                                                            | From the rule definition.                                                                |
| DB User                                                            | From the rule definition.                                                                |

| Attribute                      | Description                                                                                                                                                                                                                                         |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DB User / Group                | A single attribute and a related attribute (if exists) in a single column of the report.                                                                                                                                                            |
| DB User Group                  | From the rule definition.                                                                                                                                                                                                                           |
| Data Pattern                   | From the rule definition.                                                                                                                                                                                                                           |
| Error Code                     | From the rule definition.                                                                                                                                                                                                                           |
| Error Code / Group             | A single attribute and a related attribute (if exists) in a single column of the report.                                                                                                                                                            |
| Event type                     | From the rule definition.                                                                                                                                                                                                                           |
| Event User Name                | From the rule definition.                                                                                                                                                                                                                           |
| Exception Type                 | From the rule definition.                                                                                                                                                                                                                           |
| Field                          | From the rule definition.                                                                                                                                                                                                                           |
| Field Group                    | From the rule definition.                                                                                                                                                                                                                           |
| Field Name / Group             | A single attribute and a related attribute (if exists) in a single column of the report.                                                                                                                                                            |
| GDM_INSTALLED_POLICY_HEADER_ID | The installed policy header.                                                                                                                                                                                                                        |
| GDM_INSTALLED_POLICY_RULES_ID  | The installed policy rule.                                                                                                                                                                                                                          |
| LAST_ACCESSED                  | Last accessed.                                                                                                                                                                                                                                      |
| Min Ct                         | From the rule definition.                                                                                                                                                                                                                           |
| Net Protocol                   | From the rule definition.                                                                                                                                                                                                                           |
| Net Protocol / Group           | A single attribute and a related attribute (if exists) in a single column of the report.                                                                                                                                                            |
| Net Protocol Group             | From the rule definition.                                                                                                                                                                                                                           |
| OS User                        | From the rule definition.                                                                                                                                                                                                                           |
| OS User / Group                | A single attribute and a related attribute (if exists) in a single column of the report.                                                                                                                                                            |
| OS User Group                  | From the rule definition.                                                                                                                                                                                                                           |
| Object                         | From the rule definition.                                                                                                                                                                                                                           |
| Object Group                   | From the rule definition.                                                                                                                                                                                                                           |
| Object Name / Group            | A single attribute and a related attribute (if exists) in a single column of the report.                                                                                                                                                            |
| Object/Command Group           |                                                                                                                                                                                                                                                     |
| Pattern / XML Pattern          | From the rule definition.                                                                                                                                                                                                                           |
| Period                         | From the rule definition.                                                                                                                                                                                                                           |
| Rec Vals                       | From the rule definition.                                                                                                                                                                                                                           |
| Records Affected Threshold     | From the rule definition.                                                                                                                                                                                                                           |
| Replacement Character          | From the rule definition.                                                                                                                                                                                                                           |
| Reset Interval                 | From the rule definition.                                                                                                                                                                                                                           |
| Returned Data Threshold        | From the rule definition.                                                                                                                                                                                                                           |
| Rule Description               | From the rule definition.                                                                                                                                                                                                                           |
| Rule Position                  | Position within the policy.                                                                                                                                                                                                                         |
| Rule Type                      | One of: Access Rule (0); Exception Rule (1); Extrusion Rule (2); Fam Rule(6); Sharepoint Rule(7); Dataset Collection Profile (8); DB2 COLLECTION PROFILE (9); DB2 z/os BLOCKING PROFILE (10); IMS COLLECTION PROFILE (11); SESSION_LEVEL_RULE (12). |
| SQL Pattern                    | From the rule definition.                                                                                                                                                                                                                           |
| Server Host Group              | From the rule definition.                                                                                                                                                                                                                           |
| Server Host Name               | From the rule definition.                                                                                                                                                                                                                           |
| Server IP                      | From the rule definition.                                                                                                                                                                                                                           |
| Server IP / Group              | A single attribute and a related attribute (if exists) in a single column of the report.                                                                                                                                                            |
| Server IP Group                | From the rule definition.                                                                                                                                                                                                                           |
| Server Net Mask                | From the rule definition.                                                                                                                                                                                                                           |
| Service Name                   | From the rule definition.                                                                                                                                                                                                                           |
| Service Name / Group           | A single attribute and a related attribute (if exists) in a single column of the report.                                                                                                                                                            |
| Service Name Group             | From the rule definition.                                                                                                                                                                                                                           |
| Severity                       | From the rule definition.                                                                                                                                                                                                                           |
| Source Program / Group         | A single attribute and a related attribute (if exists) in a single column of the report.                                                                                                                                                            |
| Source Program Group           | From the rule definition.                                                                                                                                                                                                                           |
| Src App                        | From the rule definition.                                                                                                                                                                                                                           |

## Installed Rule Action entity

| Attribute      | Description                             |
|----------------|-----------------------------------------|
| Access Rule Id | Identifies the Access Rule.             |
| Action         | Block, Log or Alert.                    |
| Sequence       | Sequence of the action within the rule. |
| Template Name  | Template Name.                          |

## Installed Alert Notification entity

| Attribute             | Description                                                                     |
|-----------------------|---------------------------------------------------------------------------------|
| ALERT_ID              | Identifies the alert definition. Only available to users with the admin role.   |
| ALERT_NOTIFICATION_ID | Identifies the alert notification. Only available to users with the admin role. |
| ALERT_TYPE            | Type of alert.                                                                  |

| Attribute               | Description                                      |
|-------------------------|--------------------------------------------------|
| Alert Destination       | For example: EMAIL, SNMP, SYSLOG, CUSTM.         |
| Alert Notification Type | Type of alert from the policy rule definition.   |
| Alert User              | Receiver of the alert.                           |
| Timestamp               | Timestamp at which the alert record was created. |

## Managed units domain

The managed units domain describes the managed units and the managed unit groups in your environment. This topic describes the domain's entities and attributes. This domain cannot be used as custom domain

### Managed Unit Groups Entity

| Attribute           | Description                          |
|---------------------|--------------------------------------|
| Group Name          | The name of the managed units group. |
| Management Group ID | The ID of the managed units group.   |

### Managed Units Entity

| Attribute        | Description                                                                                  |
|------------------|----------------------------------------------------------------------------------------------|
| Host Name        | Host name of the managed unit.                                                               |
| Installed Policy | Policy installed on the managed unit.                                                        |
| Last Patch       | The last patch that was installed on the managed unit.                                       |
| Last Ping        | The last successful ping to the managed unit.                                                |
| Mac Address      | The Mac address of the managed unit.                                                         |
| Model            | The hardware model of the managed unit.                                                      |
| Online           | Whether or not the managed unit is online                                                    |
| Port             | The communication port on the managed unit.                                                  |
| Status           | The last status of the managed unit.                                                         |
| Unit IP          | The IP of the managed unit.                                                                  |
| Unit Type        | The type of the managed unit. The IP mode of the managed unit. Example: IPv4, IPv6, or dual. |
| Version          | The software running on the managed unit.                                                    |

## Parser Errors domain

This topic describes the domain's entities and attributes.

Available to roles: admin.

### Client/Server Entity

This entity describes a specific client-server connection. An instance is created each time a unique set of attributes (excluding the Timestamp) is detected.

Note: For Access Tracking only, Client/Server Entity name appears in the menu as two possible entities - Client/Server and Client/Server By Session. Client/Server By Session gets its count from the Client/Server and date conditions from the Session.

Client/Server gets its count from the Client/Server and date conditions also from the Client/Server.

If you select Client/Server, then the query is populated with ATTRIBUTE\_ID = 1. If you select Client/Server By Session, then the query is populated with MAIN\_ATTRIBUTE\_ID = 0.

| Attribute                                    | Description                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access ID                                    | A unique identifier for this unique set of client/server connection attributes. Only available to users with the admin role.                                                                                                                                                                                                                                                    |
| Analyzed Client IP                           | Applies only to encrypted traffic; when set, client IP is set to zeroes.<br>Analyzed Client IP contains the IP for encrypted sessions. For unencrypted sessions Analyzed Client IP will be the same as Client IP.                                                                                                                                                               |
| Client Host Name                             | Client host name.                                                                                                                                                                                                                                                                                                                                                               |
| Client IP                                    | Client IP address. For ASO traffic, CLIENT_IP is not the actual client IP; use the Analyzed Client IP, which is the correct IP. For Oracle ASO encrypted IPv6 traffic (local as well as remote), use the Client Host Name to identify the actual client session, due to limitations. For SSL traffic, Client IP is not the actual client IP and there is no Analyzed Client IP. |
| ClientIP / DBUser                            | Paired attribute value consisting of the client IP address and database user name.                                                                                                                                                                                                                                                                                              |
| Client IP/Src App/DB User/Server IP/Svc Name | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                             |
| Client IP/Src App/User                       | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                             |
| Client MAC                                   | Client hardware address.                                                                                                                                                                                                                                                                                                                                                        |

| Attribute                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Client OS                  | <p>Client operating system.</p> <p>For Teradata, as there is no direct information about client/server OS, instead, the data format type is used; indicating how integer data are stored during db session. This has a close relation to the platform being used and may appear as follows:</p> <p>IBM MAINFRAME // IBM mainframe data format</p> <p>HONEYWELL MAINFRAME // Honeywell mainframe data format</p> <p>AT&amp;T 3B2 // AT&amp;T 3B2 data format.</p> <p>INTEL 8086 // Intel 8086 data format (IBM PC or compatible)</p> <p>VAX // VAX data format</p> <p>AMDAHL // Amdahl data format</p>                                                                                                                                         |
| DB Protocol                | Protocol specific to the database server For example, DRDA (Db2), TNS (Oracle), or TDS (MS SQL Server).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| DB Protocol Version        | Protocol version for the DB Protocol.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| DB User Name               | Database user name: user that connected to the database, either local or remote.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Last Used                  | The timestamp of the last time the data was used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Network Protocol           | Network protocol used (such as TCP or UDP. For K-TAP on Oracle, this displays as either IPC or BEQ)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| OS User                    | OS user as reported by the database client where supported by the database type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Server Description         | Server description (if any). For example, displays cluster name of the Cloudera Data Platform.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Server Host Name           | Server host name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Server IP                  | Server IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Server IP/DB user          | Paired attribute value consisting of Server IP address and database user name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Server IP/Svc Name/DB User | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Server OS                  | <p>Server operating system.</p> <p>For Informix, the OS may appear as follows:</p> <p>IEEEM indicating Unix or JDBCIEEEI indicating WindowsDEC indicating DEC Alpha</p> <p>For Teradata, as there is no direct information about client/server OS, instead, the data format type is used; indicating how integer data are stored during db session. This has a close relation to the platform being used and may appear as follows:</p> <p>IBM MAINFRAME // IBM mainframe data format</p> <p>HONEYWELL MAINFRAME // Honeywell mainframe data format</p> <p>AT&amp;T 3B2 // AT&amp;T 3B2 data format.</p> <p>INTEL 8086 // Intel 8086 data format (IBM PC or compatible)</p> <p>VAX // VAX data format</p> <p>AMDAHL // Amdahl data format</p> |
| Server Type                | The type of database monitored, such as Dd2, Oracle, or Teradata.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Service Name               | Service name for the interaction. In some cases (AIX shared memory connections, for example), the service name is an alias that is used until the actual service is connected. In those cases, once the actual service is connected, a new session is started - so what the user experiences as a single session is logged as two sessions.<br>For Teradata, Service name contains the session logical host id value.                                                                                                                                                                                                                                                                                                                         |
| Source Program             | Source program as reported by the database client where supported by the database type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Client/ Server by session  | Client/Server by session is also a Main Entity. Access this secondary entity by clicking on the Client/Server primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Timestamp                  | The time on the collector when the client <b>first</b> connected to the server. For example, if a client is connecting to the server in the same way many days in a row this timestamp will be the time of the first connection. This may even be before the purge days of the appliance.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Timestamp Date             | Date only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Timestamp Time             | Time only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Timestamp Weekday          | Weekday only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Timestamp Year             | Year only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## Session Entity

This entity is created for each Client/Server database session.

| Attribute       | Description                                                                                                                                                                                                                                    |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access ID       | A unique identifier for this unique set of client/server connection attributes. Only available to users with the admin role.                                                                                                                   |
| Client Port     | Client port number.                                                                                                                                                                                                                            |
| Database Name   | Name of database for the session.<br>For Oracle, Database Name may contain additional and application specific information such as the currently executing module for a session that has been set in the MODULE column of the V\$SESSION view. |
| Duration (secs) | Indicates the length of time between the Session Start and the Session End (in seconds).                                                                                                                                                       |
| Global ID       | Uniquely identifies the session - access. Only available to users with the admin role.                                                                                                                                                         |
| Ignored Since   | Timestamp created when starting to ignore this session.                                                                                                                                                                                        |

| Attribute             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Inactive Flag         | <ul style="list-style-type: none"> <li>-1: Session closed by timeout.</li> <li>0 (default): Open for sessions generated by SQL package.</li> <li>1: Closed (disconnect/ logout received).</li> <li>2: Closed due to timeout on Guardium system. The session is reopened when traffic is regenerated in the session.</li> <li>3: For sessions generated from non-SQL packets.</li> </ul>                                                                                                                                                                                                                  |
| Old Session ID        | Points to the session from which this session was created. Zero if this is the first session of the connection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Original Timezone     | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00, This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |
| Process ID            | The process ID of the client that initiated the connection (not always available).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Server Port           | Server port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Session Encrypted     | Whether the session is encrypted. 0: no; 1: yes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Session End           | The time on the DB server when the session ended. Session End is also a Main Entity. Access this secondary entity by clicking on the Session primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Session End Date      | Date only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session End Time      | Time only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session End Weekday   | Weekday only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Session End Year      | Year only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session ID            | Uniquely identifies the session. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Session Ignored       | A Yes indicates that the session was ignored using the IGNORE SESSION policy action.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Session Start         | The time on the DB server when the session started. Session Start is also a Main Entity. Access this secondary entity by clicking on the Session primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Session Start Date    | Date only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Session Start Time    | Time only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Session Start Weekday | Weekday only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Session Start Year    | Year only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Terminal Id           | Terminal ID of the connection, used internally to resolve session information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Timestamp             | The time on the collector when the session information was most recently updated. Initially, a timestamp created for the first request on a client-server connection where there is not an active session in progress. Later, it is updated when the session is closed, or when it is marked inactive following an extended period of time with no observed activity. When tracking Session information, you are probably more interested in the Session Start and Session End attributes than the Timestamp attribute. If the session is closed it is the same time as the Session End.                 |
| Timestamp Date        | Date only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timestamp Time        | Time only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timestamp Weekday     | Weekday only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Timestamp Year        | Year only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| TTL                   | Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Uid Chain             | For a session reported by Unix S-TAP (K-TAP mode only), or FAM on Windows, this shows the chain of OS users, when users <code>su</code> with a different user name. For more information, see <a href="#">Linux-Unix: UID chains</a> and <a href="#">UID chain for FAM</a> .                                                                                                                                                                                                                                                                                                                             |
| Uid Chain Compressed  | The UID chain excluding the first user and the last user. For more information, see <a href="#">Linux-Unix: UID chains</a> and <a href="#">UID chain for FAM</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Parser Error entity

| Attribute    | Description |
|--------------|-------------|
| Construct Id |             |
| Count        |             |
| DB Protocol  |             |
| Description  |             |
| Error Id     |             |
| Error Type   |             |
| SQL          |             |
| Session Id   |             |
| Timestamp    |             |

## Policy Violations domain

All policy violation data, for all violations of the policy detected by the Guardium inspection engines or STAPs. This topic describes the domain's entities and attributes.

Available to roles: all

## Client/Server Entity

This entity describes a specific client-server connection. An instance is created each time a unique set of attributes (excluding the Timestamp) is detected.

Note: For Access Tracking only, Client/Server Entity name appears in the menu as two possible entities - Client/Server and Client/Server By Session. Client/Server By Session gets its count from the Client/Server and date conditions from the Session.

Client/Server gets its count from the Client/Server and date conditions also from the Client/Server.

If you select Client/Server, then the query is populated with ATTRIBUTE\_ID = 1. If you select Client/Server By Session, then the query is populated with MAIN\_ATTRIBUTE\_ID = 0.

| Attribute                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access ID                                    | A unique identifier for this unique set of client/server connection attributes. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Analyzed Client IP                           | Applies only to encrypted traffic; when set, client IP is set to zeroes.<br>Analyzed Client IP contains the IP for encrypted sessions. For unencrypted sessions Analyzed Client IP will be the same as Client IP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Client Host Name                             | Client host name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Client IP                                    | Client IP address. For ASO traffic, CLIENT_IP is not the actual client IP; use the Analyzed Client IP, which is the correct IP. For Oracle ASO encrypted IPv6 traffic (local as well as remote), use the Client Host Name to identify the actual client session, due to limitations. For SSL traffic, Client IP is not the actual client IP and there is no Analyzed Client IP.                                                                                                                                                                                                                                                                                                                                            |
| ClientIP / DBUser                            | Paired attribute value consisting of the client IP address and database user name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Client IP/Src App/DB User/Server IP/Svc Name | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Client IP/Src App/User                       | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Client MAC                                   | Client hardware address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Client OS                                    | Client operating system.<br>For Teradata, as there is no direct information about client/server OS, instead, the data format type is used; indicating how integer data are stored during db session. This has a close relation to the platform being used and may appear as follows:<br><br>IBM MAINFRAME // IBM mainframe data format<br><br>HONEYWELL MAINFRAME // Honeywell mainframe data format<br><br>AT&T 3B2 // AT&T 3B2 data format.<br><br>INTEL 8086 // Intel 8086 data format (IBM PC or compatible)<br><br>VAX // VAX data format<br><br>AMDAHL // Amdahl data format                                                                                                                                         |
| DB Protocol                                  | Protocol specific to the database server For example, DRDA (Db2), TNS (Oracle), or TDS (MS SQL Server).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| DB Protocol Version                          | Protocol version for the DB Protocol.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| DB User Name                                 | Database user name: user that connected to the database, either local or remote.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Last Used                                    | The timestamp of the last time the data was used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Network Protocol                             | Network protocol used (such as TCP or UDP. For K-TAP on Oracle, this displays as either IPC or BEQ)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| OS User                                      | OS user as reported by the database client where supported by the database type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Server Description                           | Server description (if any). For example, displays cluster name of the Cloudera Data Platform.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Server Host Name                             | Server host name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Server IP                                    | Server IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Server IP/DB user                            | Paired attribute value consisting of Server IP address and database user name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Server IP/Svc Name/DB User                   | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Server OS                                    | Server operating system.<br>For Informix, the OS may appear as follows:<br><br>IEEEM indicating Unix or JDBCIEEEI indicating WindowsDEC indicating DEC Alpha<br><br>For Teradata, as there is no direct information about client/server OS, instead, the data format type is used; indicating how integer data are stored during db session. This has a close relation to the platform being used and may appear as follows:<br><br>IBM MAINFRAME // IBM mainframe data format<br><br>HONEYWELL MAINFRAME // Honeywell mainframe data format<br><br>AT&T 3B2 // AT&T 3B2 data format.<br><br>INTEL 8086 // Intel 8086 data format (IBM PC or compatible)<br><br>VAX // VAX data format<br><br>AMDAHL // Amdahl data format |
| Server Type                                  | The type of database monitored, such as Dd2, Oracle, or Teradata.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Attribute                 | Description                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service Name              | Service name for the interaction. In some cases (AIX shared memory connections, for example), the service name is an alias that is used until the actual service is connected. In those cases, once the actual service is connected, a new session is started - so what the user experiences as a single session is logged as two sessions.<br>For Teradata, Service name contains the session logical host id value. |
| Source Program            | Source program as reported by the database client where supported by the database type.                                                                                                                                                                                                                                                                                                                               |
| Client/ Server by session | Client/Server by session is also a Main Entity. Access this secondary entity by clicking on the Client/Server primary entity.                                                                                                                                                                                                                                                                                         |
| Timestamp                 | The time on the collector when the client <b>first</b> connected to the server. For example, if a client is connecting to the server in the same way many days in a row this timestamp will be the time of the first connection. This may even be before the purge days of the appliance.                                                                                                                             |
| Timestamp Date            | Date only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                         |
| Timestamp Time            | Time only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                         |
| Timestamp Weekday         | Weekday only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                      |
| Timestamp Year            | Year only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                         |

## Incident Status Entity

Describes the status of an Incident entity.

| Attribute          | Description                                                                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status Description | One of the following:<br>OPEN - The incident has not yet been assigned to a user.<br><br>ASSIGNED - The incident has been assigned.<br><br>CLOSED - The incident is closed. |

## Incident Severity Entity

The incident severity description for an incident.

| Attribute                     | Description                                     |
|-------------------------------|-------------------------------------------------|
| Incident Severity Description | Severity code, one of :<br>INFO, LOW, MED, HIGH |

## User Entity

Identifies the Guardium user defined as an audit process results receiver.

| Attribute     | Description                                  |
|---------------|----------------------------------------------|
| EMAIL Address | Email address defined for the Guardium user. |
| First Name    | First name for the Guardium user.            |
| Last Active   | Timestamp for last activity for this user.   |
| Last Name     | Last name for the Guardium user.             |
| Login Name    | Guardium user name.                          |

## Session Entity

This entity is created for each Client/Server database session.

| Attribute         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access ID         | A unique identifier for this unique set of client/server connection attributes. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Client Port       | Client port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Database Name     | Name of database for the session.<br>For Oracle, Database Name may contain additional and application specific information such as the currently executing module for a session that has been set in the MODULE column of the V\$SESSION view.                                                                                                                                                                                                                                                                                                                                                           |
| Duration (secs)   | Indicates the length of time between the Session Start and the Session End (in seconds).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Global ID         | Uniquely identifies the session - access. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Ignored Since     | Timestamp created when starting to ignore this session.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Inactive Flag     | <ul style="list-style-type: none"> <li>• -1: Session closed by timeout.</li> <li>• 0 (default): Open for sessions generated by SQL package.</li> <li>• 1: Closed (disconnect/ logout received).</li> <li>• 2: Closed due to timeout on Guardium system. The session is reopened when traffic is regenerated in the session.</li> <li>• 3: For sessions generated from non-SQL packets.</li> </ul>                                                                                                                                                                                                        |
| Old Session ID    | Points to the session from which this session was created. Zero if this is the first session of the connection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Original Timezone | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00, This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |
| Process ID        | The process ID of the client that initiated the connection (not always available).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Attribute             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Port           | Server port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Session Encrypted     | Whether the session is encrypted. 0: no; 1: yes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Session End           | The time on the DB server when the session ended. Session End is also a Main Entity. Access this secondary entity by clicking on the Session primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Session End Date      | Date only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Session End Time      | Time only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Session End Weekday   | Weekday only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session End Year      | Year only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Session ID            | Uniquely identifies the session. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Session Ignored       | A Yes indicates that the session was ignored using the IGNORE SESSION policy action.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Session Start         | The time on the DB server when the session started. Session Start is also a Main Entity. Access this secondary entity by clicking on the Session primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Session Start Date    | Date only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Session Start Time    | Time only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Session Start Weekday | Weekday only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Session Start Year    | Year only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Terminal Id           | Terminal ID of the connection, used internally to resolve session information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Timestamp             | The time on the collector when the session information was most recently updated. Initially, a timestamp created for the first request on a client-server connection where there is not an active session in progress. Later, it is updated when the session is closed, or when it is marked inactive following an extended period of time with no observed activity. When tracking Session information, you are probably more interested in the Session Start and Session End attributes than the Timestamp attribute. If the session is closed it is be the same time as the Session End. |
| Timestamp Date        | Date only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Timestamp Time        | Time only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Timestamp Weekday     | Weekday only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timestamp Year        | Year only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| TTL                   | Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Uid Chain             | For a session reported by Unix S-TAP (K-TAP mode only), or FAM on Windows, this shows the chain of OS users, when users <code>su</code> with a different user name. For more information, see <a href="#">Linux-Unix: UID chains</a> and <a href="#">UID chain for FAM</a> .                                                                                                                                                                                                                                                                                                                |
| Uid Chain Compressed  | The UID chain excluding the first user and the last user. For more information, see <a href="#">Linux-Unix: UID chains</a> and <a href="#">UID chain for FAM</a> .                                                                                                                                                                                                                                                                                                                                                                                                                          |

## Severity Entity

The incident severity for an incident or policy violation

| Attribute            | Description                                          |
|----------------------|------------------------------------------------------|
| Severity Description | The severity code is one of:<br>INFO, LOW, MED, HIGH |

## Incident Entity

Incident entities are created by incident generation processes, or manually by assigning a policy violation to an incident.

| Attribute       | Description                              |
|-----------------|------------------------------------------|
| Category Name   | Category assigned to the incident.       |
| Incident Number | Incident number (assigned sequentially). |
| Timestamp       | Time the incident was created.           |

## Client/Server Session Entity

| Attribute                                                     | Description                                                                                         |
|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Client IP/Src App/DB User/Server IP/Svc. Name/OS User/DB Name | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> . |
| Server IP/Server Port                                         | Server IP/Server Port                                                                               |

## Policy Rule Violation Entity

This entity is created each time that a policy rule violation is logged. Not all policy rule violations are logged, see the description of the rule actions in [Policy rule actions](#). The access rule causing the violation are available in the dependent Access Rule Entity (described earlier).

| Attribute | Description |
|-----------|-------------|
|-----------|-------------|

| Attribute               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application Event Id    | Application event ID (if any - these are set using the application events API)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Application User Name   | Name of the user creating the policy rule violation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Access Rule Description | The description of the rule from its definition.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Category Name           | Category defined for the rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Classification Name     | Name of classification process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| CLS Process Run ID      | Classification process job execution ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Construct ID            | Uniquely identifies the construct in which it was referenced.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Full SQL String         | SQL string causing the policy rule violation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Incident Number         | If assigned to an incident, this is the incident number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Message Sent            | The text of the policy rule violation message that was sent.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Original Timezone       | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00, This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |
| Severity                | Severity defined for the rule (the severity of an incident to which this is assigned may be different).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Timestamp               | The time on the DB Server that the SQL triggering a policy violation was executed. Traffic must be captured with an alerting policy action to see this timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Timestamp Date          | Date only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timestamp Time          | Time only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timestamp Weekday       | Weekday only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Timestamp Year          | Year only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Total Occurrences       | Occurrence count that triggered the violation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Violation Log Id        | Uniquely identifies the violation entity. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## Application Events Entity

This entity is created each time that the system observes an Application Events API call (which sets these attribute values) or a stored procedure call that has been identified as a Custom Identification Procedure (which maps stored procedure parameters to these attributes).

| Attribute               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application Event ID    | Unique identifier for this application events entity. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Event Date              | Datetime value, set by GuardAppEvent:Start. It displays in the format yyyy-mm-dd hh:mm:ss.<br>Note: If an attempt is made to set the event date using a format other than yyyy-mm-dd, it will contain all zeroes. The time portion (hh:mm:ss) is optional, and if omitted will be 00:00:00.                                                                                                                                                                                                                                                                                                              |
| Event Release Date      | Datetime value, set by GuardAppEvent:Released. It displays in the format yyyy-mm-dd hh:mm:ss.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Event Release Type      | Type of event, set by GuardAppEvent: Released.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Event Release User Name | User name, set by GuardAppEvent: Released.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Event Release Value Num | Numeric value, set by GuardAppEvent: Released.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Event Release Value Str | String value, set by GuardAppEvent: Released.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Event Type              | Type of event, set by GuardAppEvent:Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Event User Name         | User name, set by GuardAppEvent:Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Event Value Str         | String value, set by GuardAppEvent:Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Event Value Num         | Numeric value, set by GuardAppEvent:Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Original Timezone       | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00, This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |
| Timestamp               | Created only once, when the event is logged. Do not confuse this attribute with the Event Date attribute, which can be set using an API call or from a stored procedure parameter. (See a description of the Application Events API in <a href="#">Identify_Users_with_API</a> .)                                                                                                                                                                                                                                                                                                                        |

## SQL Entity

This entity is created for each unique string of SQL. Values are replaced by question marks - only the format of the string is stored.

| Attribute     | Description                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------|
| Bind Info     | Bind information for this SQL string.                                                                           |
| Construct ID  | Uniquely identifies the construct in which the SQL appeared                                                     |
| Sql           | SQL string.                                                                                                     |
| Truncated SQL | Indicates if the SQL has been truncated or not where:<br>0 - false/no, not truncated<br>1 - true/yes, truncated |

## Command Entity

---

For each command, an entity is created for each parent node and position in which the command appears in a command construct.

| Attribute    | Description                                                                                             |
|--------------|---------------------------------------------------------------------------------------------------------|
| Command Id   | Uniquely identifies the command. Only available to users with the admin role.                           |
| Construct Id | Uniquely identifies the construct (e.g., select a from b). Only available to users with the admin role. |
| Depth        | Depth of the command in the SQL parse tree.                                                             |
| Parent       | Identifier of parent node in the parse tree.                                                            |
| SQL Verb     | Main verb in SQL command (e.g., select, insert, delete, etc.).                                          |

## Object Entity

---

An instance of this entity is created for each object in a unique schema.

| Attribute          | Description                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------|
| App Object Module1 | Uniquely identifies the application object module.                                                                |
| Construct Id       | Uniquely identifies the construct in which the object is referenced. Only available to users with the admin role. |
| Object Id          | Uniquely identifies the object. Only available to users with the admin role.                                      |
| Object Name        | Name of the object.                                                                                               |
| Schema             | Database schema for the object.<br>Note: This attribute is deprecated since it is never populated                 |

## Field Entity

---

Each time Guardium encounters a new field, it creates a field entity.

| Attribute       | Description                                                                                                                      |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------|
| Command ID      | Uniquely identifies the main command from the construct in which it was referenced. Only available to users with the admin role. |
| Construct ID    | Uniquely identifies the construct in which it was referenced. Only available to users with the admin role.                       |
| Field ID        | Uniquely identifies the field. Only available to users with the admin role.                                                      |
| Field Name      | Name of the field.                                                                                                               |
| List Clause     | Use these attributes to order complex SQL queries.                                                                               |
| Where Clause    | Example of SQL queries:                                                                                                          |
| Order by Clause | Order by                                                                                                                         |
| Having Clause   | SELECT * FROM dept_costs                                                                                                         |
| Group By Clause | WHERE dept_total >                                                                                                               |
| On Clause       | (SELECT avg FROM avg_cost)                                                                                                       |
|                 | ORDER BY department                                                                                                              |
|                 | Having                                                                                                                           |
|                 | SELECT column_name1, SUM(column_name2)                                                                                           |
|                 | FROM table_name                                                                                                                  |
|                 | GROUP BY column_name1                                                                                                            |
|                 | HAVING (numerical function condition)                                                                                            |
|                 | Group By                                                                                                                         |
|                 | SELECT column_name1, SUM(column_name2)                                                                                           |
|                 | FROM table_name                                                                                                                  |
|                 | GROUP BY column_name1                                                                                                            |
|                 | Where                                                                                                                            |
|                 | SELECT FirstName, LastName, City                                                                                                 |
|                 | FROM Users                                                                                                                       |
|                 | WHERE City = Los Angeles                                                                                                         |

| Attribute | Description                                                                                                                |
|-----------|----------------------------------------------------------------------------------------------------------------------------|
| Object ID | Uniquely identifies the object from the construct in which it was referenced. Only available to users with the admin role. |

## Policy Violations Summary domain

All policy violation data, for a summary of all violations of the policy detected by the Guardium inspection engines or STAPs. This topic describes the domain's entities and attributes.

Available to roles: all

### Client/Server Entity

This entity describes a specific client-server connection. An instance is created each time a unique set of attributes (excluding the Timestamp) is detected.

Note: For Access Tracking only, Client/Server Entity name appears in the menu as two possible entities - Client/Server and Client/Server By Session. Client/Server By Session gets its count from the Client/Server and date conditions from the Session.

Client/Server gets its count from the Client/Server and date conditions also from the Client/Server.

If you select Client/Server, then the query is populated with ATTRIBUTE\_ID = 1. If you select Client/Server By Session, then the query is populated with MAIN\_ATTRIBUTE\_ID = 0.

| Attribute                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access ID                                    | A unique identifier for this unique set of client/server connection attributes. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Analyzed Client IP                           | Applies only to encrypted traffic; when set, client IP is set to zeroes.<br>Analyzed Client IP contains the IP for encrypted sessions. For unencrypted sessions Analyzed Client IP will be the same as Client IP.                                                                                                                                                                                                                                                                                                                                                                  |
| Client Host Name                             | Client host name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Client IP                                    | Client IP address. For ASO traffic, CLIENT_IP is not the actual client IP; use the Analyzed Client IP, which is the correct IP. For Oracle ASO encrypted IPv6 traffic (local as well as remote), use the Client Host Name to identify the actual client session, due to limitations. For SSL traffic, Client IP is not the actual client IP and there is no Analyzed Client IP.                                                                                                                                                                                                    |
| ClientIP / DBUser                            | Paired attribute value consisting of the client IP address and database user name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Client IP/Src App/DB User/Server IP/Svc Name | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Client IP/Src App/User                       | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Client MAC                                   | Client hardware address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Client OS                                    | Client operating system.<br>For Teradata, as there is no direct information about client/server OS, instead, the data format type is used; indicating how integer data are stored during db session. This has a close relation to the platform being used and may appear as follows:<br><br>IBM MAINFRAME // IBM mainframe data format<br><br>HONEYWELL MAINFRAME // Honeywell mainframe data format<br><br>AT&T 3B2 // AT&T 3B2 data format.<br><br>INTEL 8086 // Intel 8086 data format (IBM PC or compatible)<br><br>VAX // VAX data format<br><br>AMDAHL // Amdahl data format |
| DB Protocol                                  | Protocol specific to the database server For example, DRDA (Db2), TNS (Oracle), or TDS (MS SQL Server).                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| DB Protocol Version                          | Protocol version for the DB Protocol.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| DB User Name                                 | Database user name: user that connected to the database, either local or remote.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Last Used                                    | The timestamp of the last time the data was used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Network Protocol                             | Network protocol used (such as TCP or UDP. For K-TAP on Oracle, this displays as either IPC or BEQ)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| OS User                                      | OS user as reported by the database client where supported by the database type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Server Description                           | Server description (if any). For example, displays cluster name of the Cloudera Data Platform.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Server Host Name                             | Server host name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Server IP                                    | Server IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Server IP/DB user                            | Paired attribute value consisting of Server IP address and database user name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Server IP/Svc Name/DB User                   | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

| Attribute                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server OS                 | <p>Server operating system.<br/>For Informix, the OS may appear as follows:</p> <p>IEEEM indicating Unix or JDBCIEEEI indicating WindowsDEC indicating DEC Alpha</p> <p>For Teradata, as there is no direct information about client/server OS, instead, the data format type is used; indicating how integer data are stored during db session. This has a close relation to the platform being used and may appear as follows:</p> <p>IBM MAINFRAME // IBM mainframe data format</p> <p>HONEYWELL MAINFRAME // Honeywell mainframe data format</p> <p>AT&amp;T 3B2 // AT&amp;T 3B2 data format.</p> <p>INTEL 8086 // Intel 8086 data format (IBM PC or compatible)</p> <p>VAX // VAX data format</p> <p>AMDAHL // Amdahl data format</p> |
| Server Type               | The type of database monitored, such as Dd2, Oracle, or Teradata.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Service Name              | Service name for the interaction. In some cases (AIX shared memory connections, for example), the service name is an alias that is used until the actual service is connected. In those cases, once the actual service is connected, a new session is started - so what the user experiences as a single session is logged as two sessions.<br>For Teradata, Service name contains the session logical host id value.                                                                                                                                                                                                                                                                                                                      |
| Source Program            | Source program as reported by the database client where supported by the database type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Client/ Server by session | Client/Server by session is also a Main Entity. Access this secondary entity by clicking on the Client/Server primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Timestamp                 | The time on the collector when the client <b>first</b> connected to the server. For example, if a client is connecting to the server in the same way many days in a row this timestamp will be the time of the first connection. This may even be before the purge days of the appliance.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Timestamp Date            | Date only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Timestamp Time            | Time only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Timestamp Weekday         | Weekday only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Timestamp Year            | Year only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## Client/Server Session Entity

| Attribute                                                     | Description                                                                                         |
|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Client IP/Src App/DB User/Server IP/Svc. Name/OS User/DB Name | A tuple group containing the named fields. For more information, see <a href="#">Tuple groups</a> . |
| Server IP/Server Port                                         | Server IP/Server Port                                                                               |

## Policy Rule Violations Summary Entity

| Attribute                 | Description                                                                                                                                   |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Access Rule Desc          |                                                                                                                                               |
| Client IP                 |                                                                                                                                               |
| Count                     |                                                                                                                                               |
| DB User                   |                                                                                                                                               |
| Policy Violation Count ID |                                                                                                                                               |
| Server IP                 |                                                                                                                                               |
| Service Name              |                                                                                                                                               |
| Session ID                | The numeric key value that Guardium assigns to uniquely identify a session. It is used to search the activities generated during the session. |
| Severity                  |                                                                                                                                               |
| Source Program            |                                                                                                                                               |
| Timestamp                 |                                                                                                                                               |
| Verdict                   |                                                                                                                                               |
| Violations Date From      |                                                                                                                                               |
| Violations Date To        |                                                                                                                                               |

## Policy Rule Violation Entity

This entity is created each time that a policy rule violation is logged. Not all policy rule violations are logged, see the description of the rule actions in [Policy rule actions](#). The access rule causing the violation are available in the dependent Access Rule Entity (described earlier).

| Attribute               | Description                                                                    |
|-------------------------|--------------------------------------------------------------------------------|
| Application Event Id    | Application event ID (if any - these are set using the application events API) |
| Application User Name   | Name of the user creating the policy rule violation.                           |
| Access Rule Description | The description of the rule from its definition.                               |
| Category Name           | Category defined for the rule.                                                 |

| Attribute           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Classification Name | Name of classification process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| CLS Process Run ID  | Classification process job execution ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Construct ID        | Uniquely identifies the construct in which it was referenced.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Full SQL String     | SQL string causing the policy rule violation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Incident Number     | If assigned to an incident, this is the incident number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Message Sent        | The text of the policy rule violation message that was sent.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Original Timezone   | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00, This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |
| Severity            | Severity defined for the rule (the severity of an incident to which this is assigned may be different).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Timestamp           | The time on the DB Server that the SQL triggering a policy violation was executed. Traffic must be captured with an alerting policy action to see this timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Timestamp Date      | Date only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timestamp Time      | Time only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timestamp Weekday   | Weekday only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Timestamp Year      | Year only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Total Occurrences   | Occurrence count that triggered the violation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Violation Log Id    | Uniquely identifies the violation entity. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## Session Entity

This entity is created for each Client/Server database session.

| Attribute           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access ID           | A unique identifier for this unique set of client/server connection attributes. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Client Port         | Client port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Database Name       | Name of database for the session.<br>For Oracle, Database Name may contain additional and application specific information such as the currently executing module for a session that has been set in the MODULE column of the V\$SESSION view.                                                                                                                                                                                                                                                                                                                                                           |
| Duration (secs)     | Indicates the length of time between the Session Start and the Session End (in seconds).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Global ID           | Uniquely identifies the session - access. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Ignored Since       | Timestamp created when starting to ignore this session.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Inactive Flag       | <ul style="list-style-type: none"> <li>• -1: Session closed by timeout.</li> <li>• 0 (default): Open for sessions generated by SQL package.</li> <li>• 1: Closed (disconnect/ logout received).</li> <li>• 2: Closed due to timeout on Guardium system. The session is reopened when traffic is regenerated in the session.</li> <li>• 3: For sessions generated from non-SQL packets.</li> </ul>                                                                                                                                                                                                        |
| Old Session ID      | Points to the session from which this session was created. Zero if this is the first session of the connection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Original Timezone   | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00, This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |
| Process ID          | The process ID of the client that initiated the connection (not always available).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Server Port         | Server port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Session Encrypted   | Whether the session is encrypted. 0: no; 1: yes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Session End         | The time on the DB server when the session ended. Session End is also a Main Entity. Access this secondary entity by clicking on the Session primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Session End Date    | Date only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session End Time    | Time only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session End Weekday | Weekday only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Session End Year    | Year only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Session ID          | Uniquely identifies the session. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Session Ignored     | A Yes indicates that the session was ignored using the IGNORE SESSION policy action.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Session Start       | The time on the DB server when the session started. Session Start is also a Main Entity. Access this secondary entity by clicking on the Session primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Session Start Date  | Date only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| Attribute             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Session Start Time    | Time only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Session Start Weekday | Weekday only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Session Start Year    | Year only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Terminal Id           | Terminal ID of the connection, used internally to resolve session information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Timestamp             | The time on the collector when the session information was most recently updated. Initially, a timestamp created for the first request on a client-server connection where there is not an active session in progress. Later, it is updated when the session is closed, or when it is marked inactive following an extended period of time with no observed activity. When tracking Session information, you are probably more interested in the Session Start and Session End attributes than the Timestamp attribute. If the session is closed it is the same time as the Session End. |
| Timestamp Date        | Date only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timestamp Time        | Time only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Timestamp Weekday     | Weekday only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Timestamp Year        | Year only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| TTL                   | Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Uid Chain             | For a session reported by Unix S-TAP (K-TAP mode only), or FAM on Windows, this shows the chain of OS users, when users <code>su</code> with a different user name. For more information, see <a href="#">Linux-Unix: UID chains</a> and <a href="#">UID chain for FAM</a> .                                                                                                                                                                                                                                                                                                             |
| Uid Chain Compressed  | The UID chain excluding the first user and the last user. For more information, see <a href="#">Linux-Unix: UID chains</a> and <a href="#">UID chain for FAM</a> .                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Severity Entity

The incident severity for an incident or policy violation

| Attribute            | Description                                          |
|----------------------|------------------------------------------------------|
| Severity Description | The severity code is one of:<br>INFO, LOW, MED, HIGH |

## Query Rewrite domain

This topic describes the domain's entities and attributes.

### Query Rewrite Log Entity

| Attribute                   | Description                            |
|-----------------------------|----------------------------------------|
| Applied QR Definition IDs   | Applied query rewrite definition ID    |
| Applied QR Definition Names | Applied query rewrite definition name. |
| Input SQL                   | Input SQL                              |
| Instance ID                 | Instance ID                            |
| Output SQL                  | Query rewrite result SQL               |
| QR Log Details              | Query rewrite detail log               |
| QR Log ID                   | Query rewrite log ID                   |
| Query Rewrite Log           | Query rewrite log                      |

## Client/Server Entity

| Attribute                                    | Description                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access Id                                    | A unique identifier for this client/server connection.                                                                                                                                                                                                                                                                                    |
| Analyzed Client IP                           | Applies only to encrypted traffic; when set, client IP is set to zeroes.<br>Analyzed Client IP has a map for CEF source. If the query used for the CEF does NOT contain the Client IP but contains the analyzed client IP, the analyzed client IP is used for the source. If both included in the query, then Client IP takes precedence. |
| Client Host Name                             | Client host name.                                                                                                                                                                                                                                                                                                                         |
| Client IP                                    | Client IP address                                                                                                                                                                                                                                                                                                                         |
| Client IP/DB User                            | Paired attribute value consisting of the client IP address and database user name.                                                                                                                                                                                                                                                        |
| Client IP/Src App/DB User/Server IP/Svc Name | Client IP address / Source Application Program / Database User Name/ Server IP address / Service Name                                                                                                                                                                                                                                     |
| Client IP/Src App/User                       | Client IP address / Source Application Program / user name                                                                                                                                                                                                                                                                                |
| Client MAC                                   | Client hardware address.                                                                                                                                                                                                                                                                                                                  |

| Attribute                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Client OS                  | <p>Client operating system.</p> <p>For Teradata, as there is no direct information about client/server OS, instead, the data format type is used; indicating how integer data are stored during db session. This has a close relation to the platform being used and may appear as follows:</p> <p>IBM MAINFRAME // IBM mainframe data format</p> <p>HONEYWELL MAINFRAME // Honeywell mainframe data format</p> <p>AT&amp;T 3B2 // AT&amp;T 3B2 data format.</p> <p>INTEL 8086 // Intel 8086 data format (IBM PC or compatible)</p> <p>VAX // VAX data format</p> <p>AMDAHL // Amdahl data format</p>                                                                                                                                                 |
| DB Protocol                | Protocol specific to the database server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| DB Protocol Version        | Protocol version for the DB Protocol.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| DB User Name               | Database user name: user that connected to the database, either local or remote.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Network Protocol           | Network protocol used (e.g., TCP, UDP, etc. Note that for K-TAP on Oracle, this displays as either IPC or BEQ)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| OS User                    | OS user account for the interaction.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Server Description         | Server description (if any).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Server Host Name           | Server Host Name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Server IP                  | Server IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Server IP/DB User          | Paired attribute value consisting of Server IP address and database user name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Server IP/Svc Name/DB User | Server IP address / Service Name / Database user name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Server OS                  | <p>Server operating system.</p> <p>For Informix, the OS may appear as follows:</p> <p>IEEEEM indicating Unix, or JDBCIEEEI indicating Windows, or DEC indicating DEC Alpha.</p> <p>For Teradata, as there is no direct information about client/server OS, instead, the data format type is used; indicating how integer data is stored during db session. This has a close relation to the platform being used and may appear as follows:</p> <p>IBM® MAINFRAME // IBM mainframe data format</p> <p>HONEYWELL MAINFRAME // Honeywell mainframe data format</p> <p>AT&amp;T 3B2 // AT&amp;T 3B2 data format.</p> <p>INTEL 8086 // Intel 8086 data format (IBM PC or compatible)</p> <p>VAX // VAX data format</p> <p>AMDAHL // Amdahl data format</p> |
| Server Type                | DB2, Oracle, Sybase, etc.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Service Name               | <p>Service name for the interaction. In some cases (AIX® shared memory connections, for example), the service name is an alias that is used until the actual service is connected. In those cases, once the actual service is connected, a new session is started - so what the user experiences as a single session is logged as two sessions.</p> <p>For Teradata, Service name contains the session logical host id value.</p>                                                                                                                                                                                                                                                                                                                     |
| Source Program             | Source program for the interaction.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Timestamp                  | Since all attributes in this entity contain static information, this timestamp is created only once, when Guardium observes a request on the defined client-server connection for the first time.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Timestamp Date             | Date only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Timestamp Time             | Time only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Timestamp Weekday          | Weekday only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Timestamp Year             | Year only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Session Entity

| Attribute       | Description                                                                                                                                                                                                                                                                      |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access Id       | A unique identifier for this client/server connection.                                                                                                                                                                                                                           |
| Client Port     | Client port number.                                                                                                                                                                                                                                                              |
| Collector Id    | The identifier of Guardium collector.                                                                                                                                                                                                                                            |
| Database Name   | <p>Name of database for the session (MSSQL or Sybase only).</p> <p>For Oracle, Database Name may contain additional and application specific information such as the currently executing module for a session that has been set in the MODULE column of the V\$SESSION view.</p> |
| Duration (secs) | The length of time between the Session Start and the Session End (in seconds).                                                                                                                                                                                                   |
| Encryption Type | The network traffic encryption type. This field is populated only for some database types. It is not an accurate indication of whether encryption is used, or the type of encryption.                                                                                            |
| Failover Flag   |                                                                                                                                                                                                                                                                                  |
| Global Id       | Uniquely identifies the session - access.                                                                                                                                                                                                                                        |
| Ignored Since   | Timestamp created when starting to ignore this session.                                                                                                                                                                                                                          |

| Attribute              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Inactive Flag          | <ul style="list-style-type: none"> <li>0: Open for sessions generated by SQL package.</li> <li>1: Closed (disconnect/ logout received).</li> <li>2: Probably closed; unclosed with no packets for a long time.</li> <li>3: For sessions generated from non-SQL packets.</li> </ul>                                                                                                                                                                                                                                                                                                                                  |
| Inspection Engine Id   | Inspection engine identifier                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Inspection Engine Name | Name of inspection engine reporting this data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Last Used              | The timestamp of the last time the data was used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Login Succeeded        | Whether or not the login succeeded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| MS/ TD SID             | Microsoft / Teradata Session ID                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Old session Id         | Points to the session from which this session was created. Zero if this is the first session of the connection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Original Timezone      | <p>The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.</p> <p>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00. This means that these events occurred 3 hours apart, but at the same respective local time (9 PM).</p> |
| Process ID             | The process ID of the client that initiated the connection (not always available).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Sender IP              | Sender's IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Server Port            | Server port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Session End            | Date and time the session ended. Session End is also a Main Entity. Access this secondary entity by clicking on the Session primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Session End Date       | Date only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Session End Time       | Time only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Session End Weekday    | Weekday only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Session End Year       | Year only from the Session End.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Session Id             | Uniquely identifies the session.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Session Ignored        | Indicates whether or not some part of the session was ignored (beginning at some point in time).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Session Start          | Date and time session started. Session Start is also a Main Entity. Access this secondary entity by clicking on the Session primary entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Session Start Date     | Date only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Session Start Weekday  | Weekday only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Session Start Year     | Year only from the Session Start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| TTL                    | Reserved for admin role use only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Terminal Id            | Terminal ID of the connection, used internally to resolve session information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Timestamp              | Initially, a timestamp created for the first request on a client-server connection where there is not an active session in progress. Later, it is updated when the session is closed, or when it is marked inactive following an extended period of time with no observed activity. When tracking Session information, you will probably be more interested in the Session Start and Session End attributes than the Timestamp attribute.                                                                                                                                                                           |
| Timestamp Date         | Date only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Timestamp Time         | Time only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Timestamp WeekDay      | Weekday only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Timestamp Year         | Year only from the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Uid Chain              | <p>For a session reported by Unix S-TAP (KTap mode only), this shows the chain of OS users, when users su with a different user name. The values that appear here vary by OS platform - for example, under AIX the string IBM IBM IBM may appear as a prefix.</p> <p>Note: For Solaris Zones, user ids may be reported instead of user names in the Uid Chain.</p>                                                                                                                                                                                                                                                  |
| Uid Chain Compressed   | Values compressed. See Uid Chain.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## Access Period Entity

| Attribute              | Description                                                                                                                                                                                                                                            |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application Event Id   | The application event ID if set from the API. These attributes appear only when the main entity for the query permits this level of detail. These are not available if either Client/Server or Session is the main entity.                             |
| Application User       | Application user name.                                                                                                                                                                                                                                 |
| Average Execution Time | The average command execution time during the period. This is for SQL statements only. It does not apply to FTP traffic.                                                                                                                               |
| Avg Execution Ack Time | The average command execution time during the period. This is for SQL statements only. It does not apply to FTP traffic.                                                                                                                               |
| Avg Records Affected   | The average number of records affected. See note at the end of the table. These attributes appear only when the main entity for the query permits this level of detail. These are not available if either Client/Server or Session is the main entity. |
| Collector Id           | The identifier of the Guardium collector.                                                                                                                                                                                                              |
| Construct Id           | Uniquely identifies a command construct (for example, select a from b). Only available to users with the admin role.                                                                                                                                   |

| Attribute                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DB2 i Current User            | DB2 i current user name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| DB2 i/z Database              | DB2 i/z database name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| DB2 i/z Program               | DB2 i/z program name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Egress Kbyte Count            | The count of egress data in Kilobytes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| F5 Ip                         | F5 IP address                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| F5 User Name                  | F5 user name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Failed Sqls                   | The number of failed SQL requests. These attributes appear only when the main entity for the query permits this level of detail. These are not available if either Client/Server or Session is the main entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| IMS PSB Name                  | IMS System Utilities - Program Specification Block (PSB) name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Ingress Kbyte Count           | The count of ingress data in Kilobytes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| instance Id                   | Uniquely identifies an instance of a construct. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Objects and Verbs             | SQL objects and commands                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Original Timezone             | The original timezone of the Guardium collector machine as of GMT/UTC offset.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Period End                    | Date and time for the end of the access period.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Period End Date               | Date only from the period end attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Period End Time               | Time only from the period end attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Period End Weekday            | Weekday only from the period end attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Period Start Date             | Date only from the period start attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Period Start Time             | Time only from the period start attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Period Start Weekday          | Weekday only from the period start attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Session Id                    | Uniquely identifies a session. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Show Seconds                  | If a the number of accesses per second is being tracked, this contains counts for each second in the access period (usually one hour).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Successful SQLs               | The number of successful SQL requests. These attributes appear only when the main entity for the query permits this level of detail. These are not available if either Client/Server or Session is the main entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Timestamp                     | Initially, the Timestamp value is set the first time that a request is observed on a client-server connection during an access period. By default, an access period is one hour long, but this can be changed by the Guardium administrator in the Inspection Engine Configuration. Thereafter, for each subsequent request, it is updated when the system updates the average execution time and the command count for this period.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Timestamp Date                | Date of the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Timestamp Time                | Time of the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Timestamp                     | Weekday of the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Timestamp Year                | Year of the timestamp.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Timestamp(microsec)           | UNIX Epoch time expressed in microseconds                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Total Records Affected        | <p>The total number of records affected. These attributes appear only when the main entity for the query permits this level of detail. These are not available if either Client/Server or Session is the main entity.</p> <p>If the Total Records Affected attribute is a character string instead of a number, that value appears here (for example, Large Results Set, or N/A).</p> <p>Records affected - Result set of the number of records which are affected by each execution of SQL statements.</p> <p>Note: The records affected option is a sniffer operation which requires sniffer to process additional response packets and postpone logging of impacted data which increases the buffer size and might potentially have a adverse effect on overall sniffer performance. Significant impact comes from really large responses. To prevent large amount of overhead associated with this operation, Guardium uses a set of default thresholds that allows sniffer to decide to skip processing operation when exceeded.</p> <p>You can use the store max_results_set_size, store max_result_set_packet_size, and store max_tds_response_packets CLI commands to set levels of granularity.</p> <p>Example of result set values:</p> <ul style="list-style-type: none"> <li>• Case 1, record affected value, positive number - this represents correct size of the result set.</li> <li>• Case 2, record affected value, -2 - This means number of records exceeded configurable limit (This could be tuned through CLI interface).</li> <li>• Case 3, record affected value, -1 - This shows any unsupported cases of packets configurations by Guardium.</li> <li>• Case 4, record affected value, -2 - If the result set is sent by streaming mode.</li> <li>• Case 5, record affected value, -2 - Intermediate result during record count to update user about current value, ends up with positive number of total records.</li> </ul> |
| Total Records Affected (Desc) | These attributes appear only when the main entity for the query permits this level of detail. These are not available if either Client/Server or Session is the main entity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Total Access                  | Total count of construct instances for this access period. Only available to users with the admin role.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Runtime Sensitive Object Identifier domain

This topic describes the entities and attributes for the Runtime Sensitive Object Identifier domain.

Available to roles: all

## Object entity

---

This entity describes the object attributes available for runtime sensitive object identifier processing.

| Attribute    | Description                   |
|--------------|-------------------------------|
| Construct Id | The related SQL construct ID. |
| Object Name  | From the rule definition.     |

## Runtime Sensitive Object Identifier entity

---

This entity describes the attributes available for runtime sensitive object identifier processing.

| Attribute           | Description                                                                                                                                                  |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Database Name       | The database for this record.                                                                                                                                |
| Database Type       | The database type.                                                                                                                                           |
| Matched Patterns    | From the rule definition. A match pattern is similar to a search pattern but uses regular expressions to match the defined pattern in any part of the value. |
| Sensitive Hit Count | The total number of hits for the matched patterns.                                                                                                           |
| Server IP           | The Guardium server IP.                                                                                                                                      |
| Timestamp           | Timestamp of this record.                                                                                                                                    |

## Related tasks

---

- [Runtime sensitive-object identification](#)

## Security Assessment Result domain

---

Records the results of vulnerability assessment processes. This topic describes the domain's entities and attributes.

Available to roles: admin

## Assessment Result Header Entity

---

This entity is created for each task in the assessment results set.

| Attribute               | Description                                                                                          |
|-------------------------|------------------------------------------------------------------------------------------------------|
| Assessment Result ID    | Identifies the assessment results set. Only available to users with the admin role.                  |
| Assessment ID           | Identifies the assessment. Only available to users with the admin role.                              |
| Task ID                 | Identifies the task within the assessment. Only available to users with the admin role.              |
| Parameter Modified Flag | Indicates if parameters modified since last run.                                                     |
| Execution Date          | Date that the assessment was run.                                                                    |
| Received By All         | Indicates whether or not these results have been received by all receivers on the distribution list. |
| Overall Score           | Overall score for the assessment.                                                                    |
| From Date               | From date for the assessment.                                                                        |
| To Date                 | To date for the assessment.                                                                          |
| Assessment Description  | Assessment name from the definition.                                                                 |
| Filter Client IP        | Clients selected: exact IP address, address with wildcards (*), or empty to select all.              |
| Filter Server IP        | Servers selected: exact IP address, address with wildcards (*), or empty to select all.              |
| Recommendation          | Recommendation returned for the task.                                                                |

## Test Result Entity

---

This entity is created for each set of test results.

| Attribute               | Description                                                                         |
|-------------------------|-------------------------------------------------------------------------------------|
| Test Result Id          | Identifies the test result. Only available to users with the admin role.            |
| Assessment Result Id    | Identifies the assessment results set. Only available to users with the admin role. |
| Test Id1                | Identifies the test.                                                                |
| Assessment Test Id      | Identifies the assessment test (task). Only available to users with the admin role. |
| Test Score              | Returned test score.                                                                |
| Report Result Id        | Identifies the report result.                                                       |
| Parameter Modified Flag | Indicates if parameters were modified since the last test.                          |
| Result Text             | Text returned by the test.                                                          |
| Test Description        | Description from the test definition.                                               |

| Attribute                         | Description                                                                                |
|-----------------------------------|--------------------------------------------------------------------------------------------|
| Recommendation                    | Recommendation returned by the test.                                                       |
| Score Description                 | Description of the score.                                                                  |
| Threshold String                  | The threshold prompt for the test (e.g. Maximum Number of Different IP's Allowed per user) |
| Severity                          | Severity assigned for the test result.                                                     |
| Category                          | Category for the test result.                                                              |
| Assessment Result data source Id1 | Identifies the test result data source.                                                    |
| Result Details                    | Details of the test.                                                                       |
| Exceptions Group Desc             | Exceptions Group Description. Populated when test is executed.                             |

## VA summary entity

| Attribute                | Description                                           |
|--------------------------|-------------------------------------------------------|
| Cumulative Fail Age      | Number of days in fail status since first run         |
| Cumulative Pass Age      | Number of days in pass status since first run         |
| Current Score            | Score of the last run                                 |
| Current Score Since      | Date when the current score became effective          |
| Data Source Name         | Name of the datasource                                |
| Db Host                  | Database host                                         |
| Db Type                  | Database type                                         |
| First Execution Datetime | Date and time on which the test was first executed    |
| First Fail Datetime      | Date and time when the test failed for the first time |
| First Pass Datetime      | Date and time when the test passed for the first time |
| Last Execution Datetime  | Last date and time the test was executed              |
| Last Fail Datetime       | Last date and time the test failed                    |
| Last Pass Datetime       | Last date and time the test passed                    |
| Port                     | Database port                                         |
| Service Name             | Database service name                                 |
| Test Description         | Description of the test                               |
| Test Id                  | ID of the test                                        |
| Timestamp                | When was this specific summary record updated         |
| VA Summary ID            | Id of the Summary record                              |

## Assessment Result CVSS info Entity

| Attribute                   | Description                 |
|-----------------------------|-----------------------------|
| CVSS Access Complexity      | CVSS Access Complexity      |
| CVSS Access Vector          | CVSS Access Vector          |
| CVSS Authentication         | CVSS Authentication         |
| CVSS Availability Impact    | CVSS Availability Impact    |
| CVSS Confidentiality Impact | CVSS Confidentiality Impact |
| CVSS Generated Date Time    | CVSS Generated Date Time    |
| CVSS Integrity Impact       | CVSS Integrity Impact       |
| CVSS Score                  | CVSS Score                  |
| CVSS Source                 | CVSS Source                 |

## Assessment Result CVE reference Entity

| Attribute            | Description          |
|----------------------|----------------------|
| CVE Reference Source | CVE Reference Source |
| Reference HREF       | Reference HREF       |
| Reference Type       | Reference Type       |

## Assessment Result Datasource Entity

This entity is identifies a datasource accessed by the assessment test.

| Attribute                        | Description                                                                              |
|----------------------------------|------------------------------------------------------------------------------------------|
| Assessment Result data source ID | Identifies a results set for a datasource. Accessible only by users with the admin role. |
| Assessment Result ID             | Identifies the result. Accessible only by users with the admin role.                     |
| DB Type                          | Database type: Oracle, MS-SQL, DB2®, Sybase, Informix®, etc.                             |
| DB Name                          | Database name.                                                                           |
| Version Level                    | Version level of the database.                                                           |
| Patch Level                      | Patch level of the database.                                                             |
| Full Version Info                | Full version information for the datasource                                              |
| Datasource name                  | Name of the datasource.                                                                  |
| Description                      | Datasource description.                                                                  |
| Host                             | Host name for the datasource.                                                            |

| Attribute    | Description                           |
|--------------|---------------------------------------|
| Port         | Port number on the host.              |
| Service Name | Service name for the datasource.      |
| User Name    | User name used for datasource access. |

## Severity Entity

---

The incident severity for an incident or policy violation

| Attribute            | Description                                          |
|----------------------|------------------------------------------------------|
| Severity Description | The severity code is one of:<br>INFO, LOW, MED, HIGH |

## Assessment Log Entity

---

This entity is created each time that an assessment is run.

| Attribute               | Description                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Assessment Log ID       | Uniquely identifies the assessment. Accessible only by users with the admin role.                                                                                                                                                                                                                                                                           |
| Timestamp               | Timestamp for the assessment.                                                                                                                                                                                                                                                                                                                               |
| Timestamp Date          | Date portion of timestamp.                                                                                                                                                                                                                                                                                                                                  |
| Timestamp Time          | Time portion of the timestamp.                                                                                                                                                                                                                                                                                                                              |
| Assessment Log Type     | Predefined, query or custom test.                                                                                                                                                                                                                                                                                                                           |
| Assessment Log Severity | The assessment test severity: Critical, Major, Minor, Cautionary, Informational. This is an ordered list of the level of severity classifications. Assessment test severity: Critical, Major, Minor, Cautionary, Informational. The highest severity is the first classification in this list. The lowest severity is the last classification in this list. |
| Assessment Result Id1   | Identifies the assessment results set.                                                                                                                                                                                                                                                                                                                      |
| Message                 | Message returned by the assessment.                                                                                                                                                                                                                                                                                                                         |
| Details                 | Details for this assessment.                                                                                                                                                                                                                                                                                                                                |

## Sniffer Buffer Usage Monitor domain

---

Inspection engine statistics. This topic describes the domain's entities and attributes.

Available to roles: none

## Sniffer Buffer Usage Entity

---

The system creates this entity at the interval set by the **store monitor buffer usage interval** CLI command (every 60 seconds by default).

| Attribute          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Timestamp          | The time the data was collected.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| % CPU Sniffer      | A normalized representation of sniffer CPU usage. For example, 50% sniffer usage on an 8-core appliance means that the sniffer is using 400% CPU (four cores).% CPU Sniffer can be used as a proxy to identify other problems, or to see if an appliance isn't at its "normal" values, indicating that something changed. For example, often if the sniffer CPU is high the analyzer queue would be higher, meaning the number of flat log requests is high. The number of flat log requests however is a more direct indicator. Higher sniffer CPU can also indicate a change in traffic volume or type.                                                                                            |
| % Mem Sniffer      | Percentage of memory that is used by the running sniffer process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| % CPU Mysql        | A normalized representation of the running MySQL CPU usage.% CPU Mysql can be used as a proxy to identify other problems, or to see if an appliance is not at its "normal" values, indicating something changed. For example, when % CPU Mysql is high the logger queue might be higher, meaning more chance of sniffer restarts. But checking for sniffer restarts is a more direct observation. % CPU Mysql can also be higher due to other non-sniffer processes running on the system like aggregation or audit processes.                                                                                                                                                                       |
| % Mem Mysql        | The percentage of total system memory that is used by the MySQL database. Provides general background information. This value goes up or down depending on usage of the system. The exact value is not important unless a problem was identified.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Sniffer Process ID | The sniffer process ID. The PID value in this column changes when the sniffer restarts.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Mem Sniffer        | Sniffer memory usage in kB. Sniffer memory usage is always greater than 0 when the sniffer is running. The memory usage increases as more data is held in the logger queue. Memory that is allocated to the sniffer is not released until the sniffer restarts.                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Time Sniffer       | Elapsed time used by sniffer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Free Buffer Space  | The percentage of free buffer space for the sniffer process. The sniffer buffer engine is only used in implementations that use SPAN ports, Network TAPs, or S-TAP PCAP. If the native S-TAP drivers are used, this value usually remains at 100%.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Analyzer Rate      | An approximate representation of the amount of data that is processed by the Analyzer/Parser per minute. The unit of data that is represented is an internal structure that is closely analogous to a packet. The maximum analyzer rate that a specific appliance can handle is a function of several variables, such as the appliance hardware, the type of data that is analyzed and parsed, and the type of rules that are used in the policy. Therefore, analyzer rate alone is not a good indicator of sniffer load, but it can be a good way to identify the busiest times of the day. The Analyzer Rate does not have a generic value that is problematic or a generic 'best practice' value. |

| Attribute                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Logger Rate                    | A rough representation of the amount of data that is processed by the logger per minute. The units here represent the parsed components of the SQL traffic that is inserted into the appliance's internal MySQL database. As with analyzer rate, the logger rate an appliance can handle depends on many factors, such as the appliance hardware, size of SQL statements that are logged, type of policy, and overall load on MySQL imposed by reports, and alerts.                                                                                                                                                                              |
| Analyzer Queue Length          | Indicates the amount of data that is in the Analyzer/Parser buffer. This value is one of the most direct indicators of sniffer performance. Ideally, the value remains at, or close to, zero. The analyzer queue might grow temporarily during temporary periods of high traffic, but should never remain elevated for more than five or six rows (5 - 6 minutes) in the Buffer Usage Monitor report. The Analyzer/Parser buffer is circular. When the analyzer goes over 80% of queue full, it starts to drop data or put it into flat log, depending on the system configuration. For more information, see <a href="#">Flat log process</a> . |
| Analyzer Total                 | Total number of messages already analyzed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Logger Queue Length            | The amount of SQL data that is in the logger buffer and waiting to be inserted into the collector's database. Similar to the analyzer queue, a consistently high amount of data in the logger queue indicates that the appliance is unable to cope with the amount of traffic that is monitored. Temporary spikes in buffered data are normal, provided the buffer is flushed within several minutes.                                                                                                                                                                                                                                            |
| Logger Total                   | Total number of messages already logged.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Session Queue Length           | The total number of open sessions that are monitored by the sniffer. This information is important because sniffer must allocate a certain amount of memory for each session that is monitored, and it cannot monitor more than 4000 simultaneous sessions.                                                                                                                                                                                                                                                                                                                                                                                      |
| Session Total                  | The overall number of sessions that were opened and closed since the last sniffer restart. Session total can be useful to correlate a spike with other statistics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Handler Data                   | Internal sniffing engine data.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Extra information              | Internal sniffing engine data.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Analyzer Lost Packets          | deprecated                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Eth0 Received                  | Messages received on the primary interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Eth0 Sent                      | Messages sent on the primary interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Logger Dbs Monitored           | List of database types currently being monitored.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Logger Packets Ignored by Rule | Packets ignored by policy rule action.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Logger Session Count           | Count of sessions logged.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Mysql Disk Usage               | The Current MySQL disk usage (percentage). High or increasing Mysql disk usage means that the appliance might be in danger of reaching or exceeding 90% full. At that point the sniffer automatically stops.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Mysql Is Up                    | Boolean indicator for internal database restart (1=was restarted, 0=not restarted).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Promiscuous Received           | Rate of received packets through the sniffing network cards (non-interface ports).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Sniffer Connections Ended      | Total number of connections that were monitored and ended since the inspection engine was restarted.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Sniffer Connections Used       | Total number of connections currently being monitored since inspection engine was restarted.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Sniffer Packets Dropped        | Packets dropped by sniffer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Sniffer Packets Ignored        | Packets ignored by sniffer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Sniffer Packets Throttled      | Total number of connections that were ignored due to throttling since inspection engine was restarted.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| System Cpu Load                | A normalized representation of total system CPU usage. System CPU load is derived from % CPU Sniffer and % CPU Mysql, plus other loads on the CPU. Since CPU load is derived from a few measurements, it does not indicate a specific problem. When higher than normal, it can indicate an underlying problem in many areas.                                                                                                                                                                                                                                                                                                                     |
| System Memory Usage            | System memory utilization.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| System Root Disk Usage         | System Root disk utilization.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| System Uptime                  | Time since last start-up.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| System Var Disk Usage          | The utilization of the /var partition. Most of files that are generated by the appliance are stored in /var.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Sessions normal                | Count of normal sessions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Sessions not opened            | Count of sessions not opened by sniffer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Sessions timeout               | Count of sessions timed-out.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Sessions ignored               | Count of sessions ignored by sniffer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Session Direct closed          | Count of sessions directly closed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Session guessed                | Count of sessions guessed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Open FDs                       | Open File Descriptors.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| DB Open FDs                    | Database open File Descriptors.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Di Rate                        | Relevant for FAM crawler traffic or other traffic that is logged in the Di tables.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Di Queue Length                | Relevant for FAM crawler traffic or other traffic that is logged in the Di tables.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Attribute         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Di Total          | Relevant for FAM crawler traffic or other traffic that is logged in the Di tables.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Di Lost Packets   | Relevant for FAM crawler traffic or other traffic that is logged in the Di tables.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Flat Log Requests | Number of requests that were flat logged. <b>Flat log requests indicate that the sniffer is dropping packets.</b> The sniffer usually drops packets due to an analyzer queue overflow problem caused by high traffic. <b>Flat log requests do not increase in a system that is working correctly.</b> If Flat log requests go over the threshold once it is a concern. Flat Log, when configured, takes the overflow from the buffer and stores it in a flat log, then inputs it later to the sniffer, with full analysis according to the policies. For more information, see <a href="#">Flat log process</a> . |

## S-TAP Status domain

This topic describes the domain's entities and attributes.

### STAP Properties entity

Note: View the S-TAP properties by creating a new report in the Query-Report Builder page. Select the main entity as S-TAP Properties and query as S-TAP Status. Some of the properties are listed in the below table.

| Attribute                 | Description                                                                                                                                          |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| # CPU                     |                                                                                                                                                      |
| Acknowledged by S-TAP     |                                                                                                                                                      |
| App Server Installed      | Whether or not an App server is installed. Yes / No                                                                                                  |
| DB2 Shm                   | Whether or not a DB2 shared memory driver is installed. Yes / No.                                                                                    |
| Encrypted?                | Whether or not communication from S-TAP is encrypted. Unencrypted / encryption type.                                                                 |
| Firewall Installed        | Whether or not a firewall is installed on the S-TAP. Yes or No.                                                                                      |
| Guardium® Hosts           | Lists the primary Guardium host, followed by all additional Guardiumhosts (for UNIX: tertiary and so on, in descending order).                       |
| Hunter DBS                | Deprecated.                                                                                                                                          |
| Ktap Installed            | Whether or not K-TAP is installed on the S-TAP. Yes / No.                                                                                            |
| Local TCP                 | Whether or not the S-TAP is running TCP locally. Yes / No.                                                                                           |
| MSS Shm                   | Whether or not MSS shared memory driver is installed. Yes / No.                                                                                      |
| Pipes                     | Whether or not a named pipes driver is installed on the S-TAP. Yes / No.                                                                             |
| Primary Host Name         | IP or hostname of the primary Guardium system receiving data from this S-TAP.                                                                        |
| Sender IP                 |                                                                                                                                                      |
| Software Tap Host         | IP or hostname of the DB hosting this S-TAP                                                                                                          |
| TEE installed             | Deprecated.                                                                                                                                          |
| Tap Version               | The S-TAP software version.                                                                                                                          |
| Timestamp                 | Timestamp of the S-TAP status.                                                                                                                       |
| DB Install Dir            | For DB2, Informix, or Oracle: the full path name for the database installation directory. For example: /home/oracle10. All other database types: NA. |
| DB Port max               | Ending port number of the range of listening ports for the database.                                                                                 |
| DB Port min               | Starting port number of the range of listening ports that are configured for the database.                                                           |
| DB Server type            | Protocol of the DB server                                                                                                                            |
| Inspection Engine Name    | Inspection Engine Name.                                                                                                                              |
| Instance Name             | The name of the database instance.                                                                                                                   |
| Port Range                | The monitored port range.                                                                                                                            |
| Sequence                  | The sequence number of the inspection engine.                                                                                                        |
| Status                    | S-TAP status. One of: Active, Inactive , Synchronizing.                                                                                              |
| Tap ID                    | Inspection engine identifier.                                                                                                                        |
| Timestamp                 | Timestamp of the report.                                                                                                                             |
| Unix Domain Socket Marker | The UNIX domain sockets marker for Oracle, MySQL and Postgres.                                                                                       |

### STAP DB server entity

| Attribute              | Description                                                                                                                                         |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| DB Exec File           | Database service executable that is monitored.                                                                                                      |
| DB Install Dir         | For DB2, Informix, or Oracle: the full path name for the database installation directory. For example: /home/oracle10. All other database types: NA |
| DB Port max            | Ending port number of the range of listening ports for the database.                                                                                |
| DB Port min            | Starting port number of the range of listening ports that are configured for the database.                                                          |
| DB Server Type         | Protocol of the DB server                                                                                                                           |
| Inspection Engine Name | Name of the inspection engine                                                                                                                       |
| Instance Name          | The name of the database instance                                                                                                                   |
| Port Range             | The monitored port range.                                                                                                                           |
| Sequence               | The sequence number of the inspection engine.                                                                                                       |
| Status                 | S-TAP status. One of: Active, Inactive , Synchronizing.                                                                                             |
| Tap ID                 | Inspection engine identifier                                                                                                                        |
| Timestamp              | Timestamp of the report.                                                                                                                            |

| Attribute                 | Description                                                    |
|---------------------------|----------------------------------------------------------------|
| Unix Domain Socket Marker | The UNIX domain sockets marker for Oracle, MySQL and Postgres. |

## S-TAP status history domain

This topic describes the domain's entities and attributes.

### STAP Properties history entity

| Attribute             | Description                                                                                                                                         |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Acknowledged by S-TAP |                                                                                                                                                     |
| App Server Installed  | Whether an App server is installed. Yes / No.                                                                                                       |
| Change Time           |                                                                                                                                                     |
| DB2 Shm               | Whether a DB2 shared memory driver is installed. Yes / No.                                                                                          |
| Encrypted?            | Whether communication from S-TAP is encrypted. Unencrypted / encryption type.                                                                       |
| Firewall Installed    | Whether a firewall is installed on the S-TAP. Yes / No.                                                                                             |
| Hunter DBS            |                                                                                                                                                     |
| Ktap Installed        | Whether K-TAP is installed on the S-TAP. Yes / No.                                                                                                  |
| Local TCP             | Whether the S-TAP is running TCP locally. Yes / No.                                                                                                 |
| MSS Shm               | Whether a MSS shared memory driver is installed on the S-TAP. Yes / No.                                                                             |
| Pipes                 | Whether a named pipes driver is installed on the S-TAP. Yes / No.                                                                                   |
| Primary Host Name     | IP or hostname of the primary Guardium system receiving data from this S-TAP.                                                                       |
| S-TAP Changed         |                                                                                                                                                     |
| Software Tap Host     | IP or hostname of the DB hosting this S-TAP.                                                                                                        |
| TEE installed         | Whether Tee is installed on the S-TAP. Yes / No.                                                                                                    |
| Tap Version           | The S-TAP software version.                                                                                                                         |
| Timestamp             | Timestamp of the status record                                                                                                                      |
| DB Install Dir        | For DB2, Informix, or Oracle: the full path name for the database installation directory. For example: /home/oracle10. All other database types: NA |
| DB Port max           | Ending port number of the range of listening ports for the database.                                                                                |
| DB Port min           | Starting port number of the range of listening ports that are configured for the database.                                                          |
| DB Server type        | Protocol of the DB server                                                                                                                           |
| Instance Name         | The name of the database instance                                                                                                                   |
| Port Range            | Range of ports monitored                                                                                                                            |
| Sequence              |                                                                                                                                                     |
| Status                | S-TAP status. One of: Active, Inactive , Synchronizing.                                                                                             |
| Tap Identifier        | Inspection engine identifier                                                                                                                        |
| Timestamp             | Timestamp of the report                                                                                                                             |

### STAP DB Server History entity

| Attribute      | Description                                                                                                                                         |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| DB Exec File   | Database service executable that is monitored.                                                                                                      |
| DB Install Dir | For DB2, Informix, or Oracle: the full path name for the database installation directory. For example: /home/oracle10. All other database types: NA |
| DB Port Max    | Ending port number of the range of listening ports for the database.                                                                                |
| DB Port Min    | Starting port number of the range of listening ports that are configured for the database.                                                          |
| DB Server type | Protocol of the DB server                                                                                                                           |
| instance Name  | The name of the database instance                                                                                                                   |
| Port Range     | Range of ports monitored                                                                                                                            |
| Sequence       |                                                                                                                                                     |
| Status         | S-TAP status                                                                                                                                        |
| Tap Identifier | Inspection engine identifier                                                                                                                        |
| Timestamp      | Timestamp of the status report                                                                                                                      |

## S-TAP Statistics domain

This topic describes the domain's entities and attributes.

Available to roles: all

### STAP statistics entity

| Attribute | Description |
|-----------|-------------|
|           |             |

| Attribute                           | Description                                                                                   |
|-------------------------------------|-----------------------------------------------------------------------------------------------|
| Activated ATAPs                     | List of A-TAPs that are activated                                                             |
| Buffer Recycled                     | How many times the S-TAP buffer has overflowed                                                |
| Erroneous ATAPs                     | A-TAPs that don't look right: activated but look deactivated, deactivated but look activated. |
| IOCTL Requests                      | Number of ioctls sent to K-TAP                                                                |
| Non-activated ATAPs                 | List of A-TAPs that are not activated                                                         |
| Software Tap Host                   | IP or hostname of the DB server                                                               |
| Stap CPU Percent                    | CPU percentage used by STAP as comes from ps                                                  |
| Stap Statistics Identifier          |                                                                                               |
| Stap Total Priority Packets Dropped | The number of priority packets dropped.                                                       |
| System CPU Idle Percent             | CPU idle percentage, as comes from ps                                                         |
| System CPU Percent                  | CPU percentage used by system, as comes from ps                                               |
| Timestamp                           | Timestamp of the statistics                                                                   |
| Total Buffer Init                   | In the K-TAP part, number of times the buffer initialized                                     |
| Total Bytes Dropped So Far          | In the K-TAP part, amount of bytes dropped                                                    |
| Total Bytes Ignored                 | In the K-TAP part, amount of bytes ignored                                                    |
| Total Bytes So Far                  | In the K-TAP part, amount of bytes captured                                                   |
| Total Response Bytes Ignored        | In the K-TAP part, amount of S2C bytes ignored                                                |

## S-TAP verification domain

This topic describes the domain's entities and attributes.

### STAP verification header entity

| Attribute                   | Description                                                     |
|-----------------------------|-----------------------------------------------------------------|
| Datasource Id               | Primary key from the mysql turbine database table – Datasources |
| IE Database Type            | Inspection Engine Database Type                                 |
| Last Verification Time      | The time at which the S-TAP verification was run.               |
| Next Verification Date Time | The time at which the next S-TAP verification should run.       |
| STAP Host                   | Host name of the server where the S-TAP is installed.           |
| STAP IP Address             | IP address of the server where the S-TAP is installed.          |
| STAP Instance Name          | Name of the S-TAP instance                                      |
| STAP Port                   | The port on the DB server that the S-TAP monitors               |
| STAP Verification HeaderID  | S-TAP verification header table primary key.                    |
| STAP Verification Result    | The result of the verification.                                 |
| STAP Verification Status    | The status of the verification.                                 |
| TAP DB Server Type          | The database server type                                        |
| Timestamp                   |                                                                 |
| Verification Scheduled      | Whether or not verification is scheduled.                       |
| Verification Type           | The type of verification: advanced or normal.                   |

### STAP verification result entity

| Attribute                  | Description                                                     |
|----------------------------|-----------------------------------------------------------------|
| Datasource Description     | The description of the datasource (from the datasources table). |
| Datasource ID              | The primary key of the datasources table.                       |
| Datasource Service Name    | Service Name running on the datasource                          |
| Datasource Severity        |                                                                 |
| Datasource Type            | Datasource type of the inspection engine being verified.        |
| STAP Database Type         | Type of database on which the S-TAP is installed.               |
| STAP Host                  | Host name of the server where the S-TAP is installed.           |
| STAP IP Address            | IP address of the server where the S-TAP is installed.          |
| STAP Instance Name         | Name of the S-TAP instance                                      |
| STAP Port                  | The port on the DB server that the S-TAP monitors               |
| STAP Verification HeaderID | S-TAP verification header table primary key.                    |
| STAP Verification Result   | The result of the verification.                                 |
| STAP Verification Status   | The status of the verification.                                 |
| STAP Verification Time     | The time of the verification.                                   |
| Timestamp                  |                                                                 |
| Verification Type          | The type of verification: advanced or normal.                   |

## Unit Utilization Levels domain

This topic describes the domain's entities and attributes.

Available to roles:

## Unit Utilization Level entity

Several unit utilization reports are provided by default at Manage > Reports > Unit Utilization, including:

- Unit Utilization: Displays the maximum unit utilization level for each unit in the given timeframe. There is a drill-down that displays details for a unit across all periods within the timeframe of the report.
- Unit Utilization Distribution: Per-unit, this report displays the percent of periods in the report timeframe with utilization levels of low, medium, and high.
- Utilization Thresholds: This predefined report displays all low and high threshold values for all unit utilization parameters.
- Unit Utilization Daily Summary: Provides a daily summary of unit utilization data.

In addition, Units Utilization Levels tracking enables users to create custom queries and reports.

Tip: Enable aliases for all custom and pre-defined reports using unit utilization data to ensure that unit utilization levels are displayed as meaningful strings instead of numbers. For example, low, medium, and high instead of 1, 2, or 3.

The list of attributes includes:

| Attribute                         | Description |
|-----------------------------------|-------------|
| Analyzer Queue                    |             |
| Analyzer Queue Level              |             |
| Free Buffer Space                 |             |
| Free Buffer Space Level           |             |
| Host Name                         |             |
| Logger Queue                      |             |
| Logger Queue Level                |             |
| Mysql Disk Usage                  |             |
| Mysql Disk Usage Level            |             |
| Number of Exceptions              |             |
| Number of Exceptions Level        |             |
| Number Of Flat Log Requests       |             |
| Number Of Flat Log Requests Level |             |
| Number Of Full SQLs               |             |
| Number Of Full SQLs Level         |             |
| Number Of Policy Violations       |             |
| Number Of Policy Violations Level |             |
| Number Of Requests                |             |
| Number Of Requests Level          |             |
| Number Of restarts                |             |
| Number Of restarts Level          |             |
| Overall Unit Utilization Level    |             |
| Percent Mysql Memory              |             |
| Percent Mysql Memory Level        |             |
| Period Start                      |             |
| Sniffer Memory                    |             |
| Sniffer Memory Level              |             |
| System CPU Load                   |             |
| System CPU Load Level             |             |
| System Var Disk Usage             |             |
| System Var Disk Usage Level       |             |

## User/Role/Application domain

Relates Guardium users, roles and applications (to report on who has access to which Guardium applications). This topic describes the domain's entities and attributes.

Available to roles: admin

### Guardium roles Entity

This entity (under User Entity) identifies a Guardium role.

| Attribute       | Description            |
|-----------------|------------------------|
| Role Identifier | ID of role identified. |
| Role            | Guardium role listed.  |

### Guardium Applications Entity

This entity (under User Entity) identifies a Guardium application.

| Attribute | Description |
|-----------|-------------|
|           |             |

| Attribute              | Description                                                                    |
|------------------------|--------------------------------------------------------------------------------|
| Application Identifier | ID of application identified.                                                  |
| Application            | Guardium application listed (for example, Query-Report, Policy Builder, etc.). |

## User Entity

---

Identifies the Guardium user defined as an audit process results receiver.

| Attribute     | Description                                  |
|---------------|----------------------------------------------|
| EMAIL Address | Email address defined for the Guardium user. |
| First Name    | First name for the Guardium user.            |
| Last Active   | Timestamp for last activity for this user.   |
| Last Name     | Last name for the Guardium user.             |
| Login Name    | Guardium user name.                          |

---

## VA Summary domain

This topic describes the domain's entities and attributes.

Available to roles: user

### VA summary entity

---

| Attribute                | Description                                           |
|--------------------------|-------------------------------------------------------|
| Cumulative Fail Age      | Number of days in fail status since first run         |
| Cumulative Pass Age      | Number of days in pass status since first run         |
| Current Score            | Score of the last run                                 |
| Current Score Since      | Date when the current score became effective          |
| Data Source Name         | Name of the datasource                                |
| Db Host                  | Database host                                         |
| Db Type                  | Database type                                         |
| First Execution Datetime | Date and time on which the test was first executed    |
| First Fail Datetime      | Date and time when the test failed for the first time |
| First Pass Datetime      | Date and time when the test passed for the first time |
| Last Execution Datetime  | Last date and time the test was executed              |
| Last Fail Datetime       | Last date and time the test failed                    |
| Last Pass Datetime       | Last date and time the test passed                    |
| Port                     | Database port                                         |
| Service Name             | Database service name                                 |
| Test Description         | Description of the test                               |
| Test Id                  | ID of the test                                        |
| Timestamp                | When was this specific summary record updated         |
| VA Summary ID            | Id of the Summary record                              |

---

## VA Tests domain

Reports on tests that are available for security assessments.

Available to roles: admin

### Assessment Tests Entity

---

This entity contains entries for available tests.

| Attribute               | Description                                                                           |
|-------------------------|---------------------------------------------------------------------------------------|
| Test Description        | Text description of the test                                                          |
| Test Type               | Type of assessment test (Observed, Predefined, Custom, Query based, CVE)              |
| Datasource Type         | Type of Datasource (DB2®, Informix®, MYSQL, ORACLE, SYBASE, etc.)                     |
| Threshold               | User defined threshold, to override the value define upon the test's creation         |
| Threshold Default Value | Default threshold that defines the success/fail criteria                              |
| Severity                | Severity of the assessment (Critical, Major, Minor, Caution, Info)                    |
| Category                | Category of the assessment (Privilege, Authentication, Configuration, Version, Other) |
| Timestamp               | Timestamp test was created                                                            |

## SQL Based Assessment Definition

---

This entity describes a SQL based assessment definition

| Attribute                | Description                                                                                                                                                                                                                          |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bind Out Var             | Optional. Determines if the entered text in SQL statement is a procedural block of code that will return a value that should be bound to an internal Guardium® variable that will be used in the comparison to the Compare to value. |
| Compare To Value         | Compare value that will be used to compare against the return value from the SQL statement using the compare operator.                                                                                                               |
| External Reference       | Reference to the Center for Internet Security (CIS) or Common Vulnerabilities and Exposures (CVE).                                                                                                                                   |
| Operator                 | Operator that will be used for the condition.                                                                                                                                                                                        |
| Recommendation Text Fail | The Recommended text for fail that will be displayed when the test fails.                                                                                                                                                            |
| Recommendation Text Pass | The Recommended text for pass that will be displayed when the test passes.                                                                                                                                                           |
| Result Text Fail         | The Result text for fail that will be displayed when the test fails.                                                                                                                                                                 |
| Result Text Pass         | The Result text for pass that will be displayed when the test passes.                                                                                                                                                                |
| Return Type              | The Return type that will be returned from the SQL statement.                                                                                                                                                                        |
| Short Description        | The short description for the assessment test.                                                                                                                                                                                       |
| SQL For Details          | A SQL Statement for Detail, a SQL statement that retrieves a list of strings to generate a detail string of Detail prefix + list of strings.                                                                                         |
| SQL                      | The SQL statement that will be executed for the test.                                                                                                                                                                                |

## Value Change domain

All changes tracked by the trigger-based value change application. This topic describes the domain's entities and attributes.

Available to roles: admin

## Monitor Values Entity

A monitor values entity is created for each insert, update or delete recorded, contains the details of the change (table name, action, SQL text, etc.).

| Attribute               | Description                                                                                                                                                                                                                                               |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Timestamp               | Date and time the change was recorded on the Guardium® appliance. This timestamp is created during the data upload operation. It is not the time that the change was recorded on the audit database. To obtain that time, use the Audit Timestamp entity. |
| Timestamp Date          | Date only from the timestamp.                                                                                                                                                                                                                             |
| Timestamp Time          | Time only from the timestamp.                                                                                                                                                                                                                             |
| Timestamp Year          | Year only from the timestamp.                                                                                                                                                                                                                             |
| Timestamp Weekday       | Weekday only from the timestamp.                                                                                                                                                                                                                          |
| Server IP               | IP address of the database server.                                                                                                                                                                                                                        |
| DB Type                 | Database type.                                                                                                                                                                                                                                            |
| Service Name            | Oracle only. Database service name.                                                                                                                                                                                                                       |
| Database Name           | DB2®, Informix®, Sybase, MS SQL Server only. Database name.                                                                                                                                                                                               |
| Audit PK                | For Sybase and MS SQL Server only. A primary key used to relate old and new values (which must be logged separately for these database types).                                                                                                            |
| Audit Login Name        | Database user name defined in the datasource.                                                                                                                                                                                                             |
| Audit Table Name        | Name of the table that changed.                                                                                                                                                                                                                           |
| Audit Owner             | Owner of the changed table.                                                                                                                                                                                                                               |
| Audit Action            | Insert, Update or Delete.                                                                                                                                                                                                                                 |
| Audit Old Value         | A comma-separated list of old values, in the format:column-name=column_value,                                                                                                                                                                             |
| Audit New Value         | A comma-separated list of new values, in the format:column-name=column_value,                                                                                                                                                                             |
| SQL Text                | Available only with Oracle 9. The complete SQL statement causing the value change.                                                                                                                                                                        |
| Triggered ID            | Unique ID (on this audit database) generated for the change.                                                                                                                                                                                              |
| Audit Timestamp         | Date and time that the trigger was executed.                                                                                                                                                                                                              |
| Audit Timestamp Date    | Date portion of Audit Timestamp.                                                                                                                                                                                                                          |
| Audit Timestamp Time    | Time portion of Audit Timestamp.                                                                                                                                                                                                                          |
| Audit Timestamp WeekDay | Day of week of the Audit Timestamp.                                                                                                                                                                                                                       |
| Audit Timestamp Year    | Year of the Audit Timestamp.                                                                                                                                                                                                                              |

| Attribute         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Original Timezone | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00, This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |

## Changed Columns Entity

This entity describes a changed column.

| Attribute           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Changed Column Name | Name of the changed column on the database.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Old Value           | Value before the change.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| New Value           | Value after the change.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Original Timezone   | The UTC offset. This is done in particular for aggregators that have collectors in different time zones and so that activities that happened hours apart do not seem as if they happened at the same time when imported to the aggregator.<br>For instance, on an aggregator that aggregates data from different time zones, you can see session start of one record that is 21:00 with original timezone UTC-02:00 and another record where session start is 21:00 with original timezone UTC-05:00, This means that these events occurred 3 hours apart, but at the same respective local time (9 PM). |

## Database Entitlement Reports

You can use database entitlement reports to verify that users have access only to the appropriate data. Your Guardium system includes predefined database entitlement reports for several database types.

Note: DB Entitlements Reports are optional components that are enabled by a product key. If these components have not been enabled, the following entitlement reports do not appear in the Custom Domain Builder, Custom Query-Report Builder, and Custom Table Builder selections.

The predefined entitlement reports are listed as follows. They appear as domain names in the Custom Domain Builder, Custom Query-Report Builder, and Custom Table Builder selections:

- Oracle DB Entitlements Domains
- MYSQL DB Entitlements Domains
- DB2® DB Entitlements Domains
- DB2 for i 6.1 and 7.1 DB Entitlements Domains
- SYBASE DB Entitlements Domains
- Informix® DB Entitlements Domains
- Microsoft SQL Server Entitlements Domains
- Netezza® DB Entitlements Domains
- Teradata DB Entitlements Domains
- PostgreSQL DB Entitlements Domains
- Azure SQL DB Entitlement Domains
- Neo4j Entitlement Domains
- Apache Cassandra Entitlement Domains
- DataStax Cassandra Entitlement Domains
- 12.1 and later Cockroach DB Entitlement Domains

See also [Entitlement Optimization](#).

## Oracle DB Entitlements

The following domains are provided to facilitate uploading and reporting on Oracle DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder, Custom Query-Report Builder, and Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports. To see entitlement reports, log on the user portal, and go to the DB Entitlements tab.

Oracle

- ORA Accnts of ALTER SYSTEM - Accounts with ALTER SYSTEM and ALTER SESSION privileges
- ORA Accnts with BECOME USER - Accounts with BECOME USER privileges
- ORA All Sys Priv and admin opt - Report showing all system privilege and admin option for users and roles
- ORA Obj And Columns Priv - Object and columns privileges granted (with or without grant option)
- ORA Object Access By PUBLIC - Object access by PUBLIC
- ORA Object privileges - Object privileges by database account not in the SYS and not a DBA role
- ORA PUBLIC Exec Priv On SYS Proc - Execute privilege on SYS PL/SQL procedures assigned to PUBL
- ORA Roles Granted - Roles granted to users and roles
- ORA Sys Priv Granted - Hierarchical report showing system privilege granted to users including recursive definitions (i.e. privileges assigned to roles and then these roles assigned to users)
- ORA SYSDBA and SYSOPER Accnts - Accounts with SYSDBA and SYSOPER privileges

For entitlements to be able to upload data from various datasources, the general requirement is that the login, used to access the database, be able to read the tables used in the query (which is hidden for all entitlements).

The following list (with comment line heading) details the minimal privileges required, in the database table (or view of the database table), for the entitlement to work.

/\* Select privilege to these tables/views is required \*/

```

grant select on sys.dba_tab_privs to sqlguard;
grant select on sys.dba_roles to sqlguard;
grant select on sys.dba_users to sqlguard;
grant select on sys.dba_role_privs to sqlguard;
grant select on sys.dba_sys_privs to sqlguard;
grant select on sys.obj$ to sqlguard;
grant select on sys.user$ to sqlguard;
grant select on sys.objauth$ to sqlguard;
grant select on sys.table_privilege_map to sqlguard;
grant select on sys.dba_objects to sqlguard;
grant select on sys.v_$pwfile_users to sqlguard;
grant select on sys.dba_col_privs to sqlguard;

```

## MYSQL DB Entitlements

---

The following domains are provided to facilitate uploading and reporting on MYSQL DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder, Custom Query-Report Builder, and Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports. To see entitlement reports, log on the user portal, and go to the DB Entitlements tab.

MYSQL: The queries ending in ".40" use the most basic version of the mysql schema (for MySQL 4.0 and beyond). The information\_schema has not changed since it was introduced in MySQL 5.0, so there is a set of \_50 queries, but no \_51 queries. The \_50 queries work for MySQL 5.0 and 5.1 and for 6.0 when it comes out, since the information\_schema is not expected to change in 6.0. The queries ending in ".502" (MYSQL502) use the new information\_schema, which contains much more information and is much more like a true data dictionary.

- MYSQL Database Privileges 40
- MYSQL User Privileges 40
- MYSQL Host Privileges 40
- MYSQL Table Privileges 40
- MYSQL Database Privileges 500
- MYSQL User Privileges 500
- MYSQL Host Privileges 500
- MYSQL Table Privileges 500
- MYSQL Database Privileges 502
- MYSQL User Privileges 502
- MYSQL Host Privileges 502
- MYSQL Table Privileges 502

For entitlements to be able to upload data from various datasources, the general requirement is that the login, used to access the database, be able to read the tables used in the query (which is hidden for all entitlements).

The following list details the minimal privileges required, in the database table (or view of the database table), for the entitlement to work.

Note: In addition to the privileges required, the user should connect to the MYSQL database to upload the data.

The entitlement queries for all MySQL versions through MySQL 5.0.1 use this set of tables: mysql.db mysql.host mysql.tables\_priv mysql.user

Beginning with MySQL 5.0.2, and for all later versions, the entitlement queries use this set of tables: information\_schema.SCHEMA\_PRIVILEGES mysql.host information\_schema.TABLE\_PRIVILEGES information\_schema.USER\_PRIVILEGES

If a datasource has a MYSQL database type, but does not have a DB name (see Datasource Definitions, the database name under Location is blank), then the uploading data will loop through all MYSQL databases the user has access to.

## DB2 DB Entitlements

---

The following domains are provided to facilitate uploading and reporting on DB2 DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder, Custom Query-Report Builder, and Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports. To see entitlement reports, log on the user portal, and go to the DB Entitlements tab.

- DB2 Column-level Privileges (SELECT, UPDATE, ETC.)
- DB2 Database -level Privileges (CONNECT, CREATE, ETC.)
- DB2 Index-level Privilege (CONTROL)
- DB2 Package-level Privileges (on code packages – BIND, EXECUTE, ETC.)
- DB2 Table-level Privileges (SELECT, UPDATE, ETC.) DB2 Privilege Summary

For entitlements to be able to upload data from various datasources, the general requirement is that the login, used to access the database, be able to read the tables used in the query (which is hidden for all entitlements).

The following list (with comment line heading) details the minimal privileges required, in the database table (or view of the database table), for the entitlement to work.

```
/* Select privilege to these tables/views is required */
```

```
GRANT SELECT ON SYSCAT.COLAUTH TO SQLGUARD;
```

```

GRANT SELECT ON SYSCAT.DBAUTH TO SQLGUARD;
GRANT SELECT ON SYSCAT.INDEXAUTH TO SQLGUARD;
GRANT SELECT ON SYSCAT.PACKAGEAUTH TO SQLGUARD;
GRANT SELECT ON SYSCAT.DBAUTH TO SQLGUARD;
GRANT SELECT ON SYSCAT.TABAUTH TO SQLGUARD;
GRANT SELECT ON SYSCAT.SCHEMAAUTH TO SQLGUARD;
GRANT SELECT ON SYSCAT.PASSTHROAUTH TO SQLGUARD;

DB2 z/OS entitlements
The following domains are provided to facilitate uploading and reporting on DB2 for z/OS DB Entitlements.

DB2 zOS Executable Object Prvts Granted To PUBLIC
DB2 zOS Object Prvts Granted To PUBLIC
DB2 zOS System Prvts Granted To GRANTEE -V8
DB2 zOS System Prvts Granted To GRANTEE -V9
DB2 zOS System Prvts Granted To GRANTEE -V10 Up
DB2 zOS Database Prvts Granted To GRANTEE
DB2 zOS Schema Prvts Granted To GRANTEE -V9 Up
DB2 zOS Schema Prvts Granted To GRANTEE -V8 Only
DB2 zOS Database Resource Granted To GRANTEE
DB2 zOS Object Prvts Granted To GRANTEE
DB2 zOS System Prvts Granted With GRANT -V8
DB2 zOS System Prvts Granted With GRANT -V9
DB2 zOS System Prvts Granted With GRANT -V10 Up
DB2 zOS Database Resource Granted To PUBLIC
DB2 zOS Schema Prvts Granted To PUBLIC
DB2 zOS Database Prvts Granted To PUBLIC
DB2 zOS System Prvts Granted To PUBLIC -V10 Up
DB2 zOS System Prvts Granted To PUBLIC -V9
DB2 zOS System Prvts Granted To PUBLIC -V8
DB2 zOS Object Prvts Granted With GRANT
DB2 zOS Database Resource Granted With GRANT
DB2 zOS Schema Prvts Granted With GRANT-V8 Only
DB2 zOS Schema Prvts Granted With GRANT-V9 Up
DB2 zOS Database Prvts Granted With GRANT

```

## DB2 for i 6.1 and 7.1 DB Entitlements

---

The following domains are provided to facilitate uploading and reporting on DB2 for i DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder, Custom Query-Report Builder, and Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports. To see entitlement reports, log on the user portal, and go to the DB Entitlements tab.

Use the script, gdmmonitor-db2-IBMi.sql, to detail the minimal privileges required, in the database table (or view of the database table), in order for the entitlement to work.

Object privileges granted to grantee (Object type: Schema, Table, View, Package, Routine, sequence, column, global variable, and XML schema)

Object privileges granted to PUBLIC (Object type: Schema, Table, View, Package, Routine, sequence, column, global variable, and XML schema)

Executable Objects privileges granted to PUBLIC (Object type: package and Routine)

Object privileges granted to grantee with GRANT OPTION (Object type: Schema, Table, View, Package, Routine, sequence, column, global variable, and XML schema)

All of the object privileges exclude default system schemas from a predefined Guardium group called "DB2 for i exclude system schemas - entitlement report". Please add to this group for schema that should be excluded.

## SAP Hana Entitlements

---

The following domains are provided to facilitate uploading and reporting on SAP Hana Entitlements.

- SAP Application Access
- SAP HANA Analytical priv granted to grantee
- SAP HANA App Privilege granted to grantee
- SAP HANA Sys priv granted to grantee
- SAP HANA DB Object priv granted to grantee
- SAP HANA Exec Objects priv granted to PUBLIC
- SAP HANA Object priv granted to grantee with GRANT OPTION
- SAP HANA Object privileges granted to PUBLIC
- SAP HANA Role granted to grantee

Use the script, gdmonitor-SAP-Hana.sql, to detail the minimal privileges required, in the database table (or view of the database table), for the entitlement to work.

For more information on running a database entitlement report, see [Running database entitlement reports](#).

## SYBASE DB Entitlements

---

The following domains are provided to facilitate uploading and reporting on SYBASE DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder, Custom Query-Report Builder, and Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports. To see entitlement reports, log on the user portal, and go to the DB Entitlements tab.

- SYBASE System Privilege and Roles Granted to User including Grant option
- SYBASE Role Granted to User and System Privileges Granted to user and role including Grant option
- SYBASE Object Access by Public
- SYBASE Execute Privilege on Procedure, function assigned To Public
- SYBASE Accounts with System or Security Admin Roles
- SYBASE Object and Columns Privilege Granted with Grant option
- SYBASE Role Granted To User

For entitlements to be able to upload data from various datasources, the general requirement is that the login, used to access the database, be able to read the tables used in the query (which is hidden for all entitlements).

The following list (with comment line heading) details the minimal privileges required, in the database table (or view of the database table), for the entitlement to work.

```
/* Select privilege to these tables/views is required */
```

```
/* These are required on MASTER database */
```

```
grant select on master.dbo.syslogins to sqlguard
```

```
grant select on master.dbo.syslogins to sqlguard
```

```
grant select on master.dbo.syssrvroles to sqlguard
```

```
/*These are required on every database, including MASTER */
```

```
grant select on sysprotects to sqlguard
```

```
grant select on sysusers to sqlguard
```

```
grant select on sysobjects to sqlguard
```

```
grant select on sysroles to sqlguard
```

If a datasource has a SYBASE database type, but does not have a DB name (see Datasource Definitions, the database name under Location is blank), then the uploading data will loop through all SYBASE databases the user has access to.

## SYBASE IQ Entitlements

---

Supported version: sybase IQ 15 and above.

The following custom table definitions are created to upload data: (You can ignore the id.)

- 139 | Sybase IQ Object Privileges By DB User
- 140 | Sybase IQ Object Privileges By Group
- 141 | Sybase IQ System Authority And Group Granted To User
- 142 | Sybase IQ System Authority And Group Granted To User And Group
- 143 | Sybase IQ Object Access By Public
- 144 | Sybase IQ Exec priv on proc func to PUBLIC
- 145 | Sybase IQ User Group With DBA Perms Admin etc
- 146 | Sybase IQ Table View priv granted with grant
- 147 | Sybase IQ Group granted to user and group
- 148 | Sybase IQ Login policy for user group with login

Corresponding query/reports are as follows: (You can ignore the id.)

- 597 | Sybase IQ Object Privileges By DB User
- 598 | Sybase IQ Object Privileges By Group
- 599 | Sybase IQ System Authority And Group Granted To User
- 600 | Sybase IQ System Authority And Group Granted To Users And Groups Grantee

- 601 | Sybase IQ Object Access By Public
- 602 | Sybase IQ Execute Privilege On Procedure and Function To PUBLIC
- 603 | Sybase IQ User Group With DBA/Perms Admin/User Admin/Remote DBA database authority
- 604 | Sybase IQ Table View Priv Granted With Grant
- 605 | Sybase IQ Group Granted To User And Group
- 606 | Sybase IQ Login Policy For User And Group With Login Option Setting

They can be found under db entitlements with the others.

---

Description of each - some of them are self explained. some may need a few extra words:

```
1 /*
Object privileges by database user.

Object include: Table, views, procedure and functions.

These are privilege granted to users only, not including group or membership in group.

*/
2. /*
Object privileges by group.

Object include: Table, views, procedure and functions.

These are privilege granted to group only.

*/
3 /* System Authority And Group Granted To Users.

*/
4 /* System Authority And Group Granted To Users And Groups Grantee.

*/
5 /* object access by public.

Including Tables, Views, Functions and Procedures

*/
6 /* Execute privilege on procedures and functions granted to PUBLIC:

*/
7 /* Users and groups with DBA, Perms Admin, User Admin or Remote DBA database authority.

*/
8 /* Tables and Views privileges granted with grant option to users and groups.

Note, this is the only grant option type allow in Sybase IQ. Routines cannot be grant with grant option.

*/
9 /* Group granted to users and group.

*/
10 /* Login policy assigned to user and group with login option setting */
```

## How to use GuardAPI to add a datasource to Sybase IQ reports

---

How to use GuardAPI to add a datasource to each of the Sybase IQ reports and how to execute them.

See the examples below on how to add a datasource to each of the new reports and then execute each report.

Add a datasource for all Sybase IQ Entitlement Reports

```
grdapicreate_datasource type="Sybase IQ" user=ent password=Guardium123 host=9.70.144.152 name="Sybase IQ entitlement6"
shared=true owner=admin application=CustomDomain port=2638 dbName=sn5qpuff
```

Add a datasource to all Sybase IQ Entitlement Reports

```
grdapicreate_datasourceRef_by_name application=CustomTables objName="Sybase IQ Exec priv on proc func to
PUBLIC"datasourceName="Sybase IQ entitlement 6"
grdapicreate_datasourceRef_by_name application=CustomTablesobjName="Sybase IQ Group granted to user and group"
datasourceName="Sybase IQ entitlement 6"
grdapicreate_datasourceRef_by_name application=CustomTablesobjName="Sybase IQ Login policy for user group with
login"datasourceName="Sybase IQ entitlement 6"
grdapicreate_datasourceRef_by_name application=CustomTablesobjName="Sybase IQ Object Access By Public" datasourceName="Sybase
IQ entitlement 6"
grdapicreate_datasourceRef_by_name application=CustomTablesobjName="Sybase IQ Object Privileges By DB User"
datasourceName="Sybase IQ entitlement 6"
```

```

grdapi create_datasourceRef_by_name application=CustomTablesobjName="Sybase IQ Object Privileges By Group"
datasourceName="Sybase IQ entitlement 6"
grdapi create_datasourceRef_by_name application=CustomTablesobjName="Sybase IQ System Authority And Group Granted To
User"datasourceName="Sybase IQ entitlement 6"
grdapi create_datasourceRef_by_name application=CustomTablesobjName="Sybase IQ System Authority And Group Granted To User And
Group"datasourceName="Sybase IQ entitlement 6"
grdapi create_datasourceRef_by_name application=CustomTablesobjName="Sybase IQ Table View priv granted with
grant"datasourceName="Sybase IQ entitlement 6"
grdapi create_datasourceRef_by_name application=CustomTablesobjName="Sybase IQ User Group With DBA Perms Admin
etc"datasourceName="Sybase IQ entitlement 6"

```

Execute ALL SybaseIQ Entitlement Reports

```

grdapi upload_custom_data tableName=SYBASEIQ_EXEC_PRIV_ON_PROC_FUNC_TO_PUBLIC
grdapi upload_custom_data tableName=SYBASEIQ_GROUP_GRANTED_TO_USER_AND_GROUP
grdapi upload_custom_data tableName=SYBASE_OBJ_COL_PRIVS_GRANTED_WITH_GRAN
grdapi upload_custom_data tableName=SYBASEIQ_OBJECT_ACCESS_BY_PUBLIC
grdapi upload_custom_data tableName=SYBASEIQ_OBJECT_PRIVS_BY_DB_USER
grdapi upload_custom_data tableName=SYBASEIQ_OBJECT_PRIVILEGES_BY_GROUP
grdapi upload_custom_data tableName=SYBASEIQ_SYSTEM_AUTHORITY_AND_GROUP_GRANTED_TO_USER grdapi upload_custom_data
tableName=SYBASEIQ_SYSTEM_AUTHORITY_AND_GROUP_GRANTED_TO_USER_AND_GROUP grpapi upload_custom_data
tableName=SYBASEIQ_TABLE_VIEWS_PRIV_GRANTED_WITH_GRANT grpapi upload_custom_data
tableName=SYBASEIQ_USER_GROUP_WITH_DB_PERMS_ADMIN_ETC

```

## Informix DB Entitlements

---

The following domains are provided to facilitate uploading and reporting on Informix DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder, Custom Query-Report Builder, and Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports. To see entitlement reports, log on the user portal, and go to the DB Entitlements tab.

- Informix Object Privileges by database account not including system account and roles
- Informix database level privileges, roles and language granted to user including grant option
- Informix database level privileges, roles and language granted to user and role including grant option
- Informix Object Grant to Public
- Informix Execute Privilege on Informix procedure and function granted to Public
- Informix Account with DBA Privilege Informix Object and columns privileges granted with Grant option
- Informix Role Granted To User and Role

For entitlements to be able to upload data from various datasources, the general requirement is that the login, used to access the database, be able to read the tables used in the query (which is hidden for all entitlements). The following list (with comment line heading) details the minimal privileges required, in the database table (or view of the database table), in order for the entitlement to work.

```
/* Select privilege to these tables/views is required */
```

Since all users have sufficient privileges for system catalog SELECT privileges, there is no need to grant privilege to any user. Informix doesn't seem to like granting system catalog to users. The grant below would normally be used. But in this case they are not required.

```

grant select on systables to sqlguard;
grant select on systabauth to sqlguard;
grant select on sysusers to sqlguard;
grant select on sysroleauth to sqlguard;
grant select on syslangauth to sqlguard;
grant select on sysroutinelangs to sqlguard;
grant select on sysprocauth to sqlguard;
grant select on sysprocedures to sqlguard;
grant select on syscolauth to sqlguard;

```

If a datasource has a Informix database type, but does not have a DB name (see Datasource Definitions, the database name under Location is blank), then the uploading data will loop through all Informix databases the user has access to.

## Microsoft SQL Server 2005 and later DB Entitlements

---

The following domains are provided to facilitate uploading and reporting on Microsoft SQL Server 2005 and later DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder, Custom Query-Report Builder, and Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports. To see entitlement reports, log on the user portal, and go to the **DB Entitlements** tab.

Note: Objects in Dynamic query Strings will NOT be shown in xxx\_DEPENDENCIES. An object in an EXECUTE IMMEDIATE SQL string called by a stored program unit does not show dependency. This query exclude schema owner defined in group ID 202 "Dependencies\_exclude\_schema-MSSQL". User has the ability to add or subtract schema name from this group for the dependencies query.

- Microsoft SQL Server Object privileges by database account not including default system user.
- Microsoft SQL Server Role/System privileges granted To User
- Microsoft SQL Server Role/System Privilege granted to user and role including grant option
- Microsoft SQL Server Object access by PUBLIC
- Microsoft SQL Server Execute Privilege on System Procedures and functions to PUBLIC
- Microsoft SQL Server Database accounts of db\_owner and db\_securityadmin Role

- Microsoft SQL Server Server account of sysadmin, serveradmin and security admin /\* only run against MASTER database \*/
- Microsoft SQL Server Object and columns privileges granted with grant option
- Microsoft SQL Server Role granted to user and role.

For entitlements to be able to upload data from various datasources, the general requirement is that the login, used to access the database, be able to read the tables used in the query (which is hidden for all entitlements).

The following list (with comment line heading) details the minimal privileges required, in the database table (or view of the database table), in order for the entitlement to work.

```
/* Select privilege to these tables/views is required */

/*These are required on MASTER database */

grant select on sys.server_principals to sqlguard

/*These are required on every databases including MASTER */

grant select on sys.database_permissions to sqlguard
grant select on sys.database_principals to sqlguard
grant select on sys.all_objects to sqlguard
grant select on sys.database_role_members to sqlguard
grant select on sys.columns to sqlguard
```

If a datasource has a MSSQL database type, but does not have a DB name (see Datasource Definitions, the database name under Location is blank), then the uploading data will loop through all MSSQL databases the user has access to.

## Netezza DB Entitlements

---

The following domains are provided to facilitate uploading and reporting on Netezza DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder, Custom Query-Report Builder, and Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports. To see entitlement reports, log on the user portal, and go to the **DB Entitlements** tab.

Note: There is no DB error text translation for Netezza. The error appears in the exception description. Users can clone/add a report with the exception description for Netezza as needed.

- Netezza Obj Prvs by DB Username - Object privileges with or without grant option by database username excluding ADMIN account.
- Netezza Admin Prvs by DB Username - Admin privileges with or without grant option by database username excluding ADMIN account.
- Netezza Group /Role Granted To User - Group (Role) granted to user
- Netezza Obj Prvs By Group - Object privileges with or without grant option by GROUP excluding PUBLIC.
- Netezza Admin Prvs By Group - Admin privileges with or without grant option by GROUP excluding PUBLIC.
- Netezza Admin Prvs By DB Username, Group - Admin privileges with or without grant option by database username, group excluding ADMIN account and PUBLIC group.
- Netezza Obj Prvs Granted - Object privileges granted with or without grant option to PUBLIC.
- Netezza Admin Prvs Granted - Admin privileges granted with or without grant option to PUBLIC.
- Netezza Global Admin Priv To Users and Groups - Global admin privilege granted to users and groups excluding ADMIN account.
- Netezza Global Obj Priv To Users and Groups - Global object privilege granted to users and groups excluding ADMIN account.

For entitlements to be able to upload data from various datasources, the general requirement is that the login, used to access the database, be able to read the tables used in the query (which is hidden for all entitlements).

The following list (with comment line heading) details the minimal privileges required, in the database table (or view of the database table), for the entitlement to work.

```
/* Select privilege to these tables/views is required */

/* This script must be run from the system database */

GRANT SELECT ON SYSTEM VIEW TO sqlguard;
GRANT LIST ON DATABASE TO sqlguard;
GRANT LIST ON USER TO sqlguard;
GRANT LIST ON GROUP TO sqlguard;
GRANT SELECT ON _V_CONNECTION TO sqlguard;
```

For Netezza entitlement queries, it is recommended to connect to SYSTEM database, especially when granting the privilege to the user who is going to run these reports. The granting privilege MUST take place from SYSTEM database or else the granted privilege will only take place on one particular database. When the granted privilege takes place from SYSTEM database, a special feature will allow the granted privilege to carry through to all the databases.

## Teradata DB Entitlements

---

The following domains are provided to facilitate uploading and reporting on Teradata DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder, Custom Query-Report Builder, and Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports. To see entitlement reports, log on the user portal, and go to the **DB Entitlements** tab.

- Teradata Object privileges by database account not including default system users.
  - Teradata System privileges and roles granted to users including grant option.
  - Teradata Roles granted to users and roles including grant option.
  - Teradata Role granted to users and roles. System privileges granted to users and roles including grant option.
  - Teradata Objects and System privileges granted to public. Note role cannot be granted to public in Teradata.
  - Teradata Execute privileges on system database objects to public.
  - Teradata System admin, Security admin privileges granted to user and role.
- Note: There are no such role as System or Security admin in Teradata. User must create their own roles. These are some important system privileges that would normally not be granted to normal user: ABORT SESSION, CREATE DATABASE, CREATE PROFILE, CREATE ROLE,CREATE USER, DROP DATABASE, DROP PROFILE, DROP ROLE, DROP USER, MONITOR RESOURCE, MONITOR SESSION, REPLICATION OVERRIDE, SET SESSION RATE, SET RESOURCE RATE.
- Teradata Object privileges granted with granted option to users. Not including DBC and grantee = 'All'.

For entitlements to be able to upload data from various datasources, the general requirement is that the login, used to access the database, be able to read the tables used in the query (which is hidden for all entitlements).

The following list (with comment line heading) details the minimal privileges required, in the database table (or view of the database table), in order for the entitlement to work.

```
/* Select privilege to these tables/views is required */
GRANT SELECT ON DBC.AllRights TO sqlguard;
GRANT SELECT ON DBC.Tables TO sqlguard;
GRANT SELECT ON DBC.AllRoleRights TO sqlguard;
GRANT SELECT ON DBC.RoleMembers TO sqlguard;
```

## PostgreSQL DB and PostgreSQL EDB Entitlements

---

The following domains are provided to facilitate uploading and reporting on PostgreSQL DB and PostgreSQL EDB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder, Custom Query-Report Builder, and Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports. To see entitlement reports, log on the user portal, and go to the **DB Entitlements** tab.

There are seven entitlement custom domains/queries/reports for PostgreSQL. They are as follows (each is listed with Report name, description, note):

- PostgreSQL Priv On. Databases Granted To Public User Role With Or Without Granted Option. Privilege on databases granted to public, user and role with or without granted option. Run this on any database, ideally PostgreSQL.
- PostgreSQL Priv On Language Granted To Public User Role With Or Without Granted Option. Privilege on Language granted to public, user and role with or without granted option. Run this per database.
- PostgreSQL Priv On Schema Granted To Public User Role With Or Without Granted Option. Privilege on Schema granted to public, user and role with or without granted option. Run this per database.
- PostgreSQL Priv On Tablespace Granted To Public User Role With Or Without Granted Option. Privilege on Tablespace granted to public, user and role with or without granted option. Run this on any database, ideally PostgreSQL.
- PostgreSQL Role Or User Granted To User Or Role (9.4 and below. For PostgreSQL DB only). Role or User granted to user or role including grant option. Run this once in any database. Ideally PostgreSQL.
- PostgreSQL Role Or User Granted To User Or Role (9.5 and above). Role or User granted to user or role including grant option. Run this once in any database. Ideally PostgreSQL.
- PostgreSQL Super User Granted To User Or Role. Super user granted to user or role. Run this once in any database. Ideally PostgreSQL.
- PostgreSQL Sys Privils Granted To User And Role. System privileges granted to user and role. Run this once in any database. Ideally PostgreSQL.
- PostgreSQL Table View Sequence and Function privs Granted To Public. Tables, Views, Sequence and Functions privileges granted to public. Run this per database. Run this per database.
- PostgreSQL Table View Sequence and Function Privils Granted With Grant Option. Tables, Views, Sequence and Functions privileges granted to user and role with grant option only. Exclude PostgreSQL account.
- PostgreSQL Table View Sequence Function Privils Granted To Roles. Tables, Views, Sequence and Functions privileges granted to roles. Not including public. Run this per database.
- PostgreSQL Table Views Sequence and Functions Privils Granted To Login. Tables, Views, Sequence and Functions privileges granted to logins. Not including postgres system user. Run this per database.

Note: As of version 8.3.6, PostgreSQL does not support grant admin option to public. There is only function, no store procedure. There is no support for column grant, only table grant. Public is a group, not user. Public does not show up in pg\_roles. The only privileges need to run all these queries is: GRANT CONNECT ON DATABASE PostgresSQL TO username;

For entitlements to be able to upload data from various datasources, the general requirement is that the login, used to access the database, be able to read the tables used in the query (which is hidden for all entitlements).

The following list (with comment line heading) details the minimal privileges required, in the database table (or view of the database table), for the entitlement to work.

```
/* Select privilege to these tables/views is required */
/*This is required on POSTGRES database*/
grant connect on database postgres to sqlguard;

/*These are required on every database, including POSTGRES (By default these are already granted to PUBLIC) */
grant select on pg_class to sqlguard;
```

```
grant select on pg_namespace to sqlguard;
grant select on pg_roles to sqlguard;
grant select on pg_proc to sqlguard;
grant select on pg_auth_members to sqlguard;
grant select on pg_language to sqlguard;
grant select on pg_tablespace to sqlguard;
grant select on pg_database to sqlguard;
```

If a datasource has a PostgreSQL database type, but does not have a DB name (see Datasource Definitions, the database name under Location is blank), then the uploading data will loop through all PostgreSQL databases the user has access to.

## Azure SQL DB Entitlements

---

The following domains are provided to facilitate uploading and reporting on Oracle DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder, Custom Query-Report Builder, and Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports.

- Azure SQL Database Role granted to user and role
- Azure SQL Database Object / Column privileges granted with grant option
- Azure SQL Database Accounts with db\_owner / db\_securityadmin role
- Azure SQL Database Role / System privileges granted to user and role
- Azure SQL Database Object privileges granted to PUBLIC
- Azure SQL Database Privileges on system procedures / functions granted to PUBLIC
- Azure SQL Database Object privileges granted to user and role

## Neo4j DB Entitlements

---

The following domains are provided to facilitate uploading and reporting on Oracle DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder, Custom Query-Report Builder, and Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports.

- Neo4j roles granted to users
- Neo4j privileges for built-in roles
- Neo4j privileges for user roles (excluding built-in roles)
- Neo4j privileges denied to user roles

## Apache Cassandra DB Entitlements

---

The following domains are provided to facilitate uploading and reporting on Apache Cassandra DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder, Custom Query-Report Builder, and Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports.

- Apache Cassandra SuperUser role
- Apache Cassandra Roles granted with AUTHORIZE permission
- Apache Cassandra Role granted to user role
- Apache Cassandra DB Object privileges granted to grantee

## DataStax Cassandra DB Entitlements

---

The following domains are provided to facilitate uploading and reporting on DataStax Cassandra DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder, Custom Query-Report Builder, and Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports.

- DataStax Cassandra SuperUser Role
- DataStax Cassandra Object privileges granted with grant option
- DataStax Cassandra Role granted to User Role
- DataStax Cassandra DB Object privileges granted to grantee

## Cockroach DB Entitlements

---

12.1 and later The following domains are provided to facilitate uploading and reporting on Cockroach DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder, Custom Query-Report Builder, and Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports.

- CockroachDB Create privilege granted to User or Role
- CockroachDB Super User granted to User or Role
- CockroachDB Sys privileges granted to User or Role

- CockroachDB privileges granted to grantee (Cockroach DB version 24.1 and later)
- CockroachDB privileges granted to grantee (pre Cockroach DB version 24.1)  
Note: This entitlement is applicable for database versions earlier than 24.1.
- CockroachDB privileges granted with GRANT option

## Custom Domains

Custom domains allow for user defined domains and can define any tables of data uploaded to your Guardium system.

The usage for these custom entitlement (privileges) domains are for entitlement reports which are found if logged in as a user. To see these reports, go to the user tab DB Entitlements.

A number of custom domains have been predefined. You can use them to import data.

If you create a custom domain, and do not see it immediately after in the Custom Query-Report Builder, log out of the UI and log in again.

For details on using custom tables and custom domains, see [External data correlation](#).

## [Custom] Access

This domain contains all of the same entities as the standard Data Access domain. It is provided as a custom domain to allow additional user-defined domains to be built including information from this domain and any custom tables that have been uploaded by the user. [Custom]Access domain is meant to be cloned. This domain is updated on each version therefore is not advisable to create reports on this domain. For a description of the entities included in the Access domain, see the Access domain description in the Domains topic.

## S-TAP Info (Central Manager)

Report: See S-TAP Reports. On a Central Manager, an additional report, S-TAP Info, is available. This report monitors S-TAPs of the entire environment. Upload this data using the Custom Table Builder.

S-TAP info is a predefined custom domain which contains the S-TAP Info entity and is not modifiable.

When defining a custom query, go to upload page and click Check/Repair to create the custom table in CUSTOM database, otherwise save query will not validate it. This table loads automatically from all remote sources. A user cannot select which remote sources are used - it pulls from all of them.

Based on this custom table and custom domain, there are two reports:

Enterprise S-TAP view shows, from the Central Manager, information on an active S-TAP on a collector and/or managed unit (If there are duplicates for the same S-TAP engine, one being active and one being inactive, then the report will only use the active).

Detailed Enterprise S-TAP view shows, from the Central Manager, information on all active and passive S-TAPs on all collectors and/or managed units.

If the Enterprise S-TAP view and Detailed Enterprise S-TAP view look the same, it is because there only one S-TAP on one managed unit being displayed. The Detailed Enterprise S-TAP view would look different if there is more S-TAPs and more managed units involved.

These two reports can be chosen from the TAP Monitor tab of a standalone system, but they will display no information.

## DB Entitlement Domains

Along with authenticating users and restricting role-based access privileges to data, even for the most privileged database users, there is a need to periodically perform entitlement reviews, the process of validating and ensuring that users only have the privileges required to perform their duties. This is also known as database user rights attestation reporting.

Use Guardium's predefined database entitlement (privilege) reports (for example) to see who has system privileges and who has granted these privileges to other users and roles. Database entitlement reports are important for auditors tracking changes to database access and to ensure that security holes do not exist from lingering accounts or ill-granted privileges.

DB Entitlement Reports use the Custom Domain feature to create links between the external data on the selected database with the internal data of the predefined entitlement reports. See Database Entitlements Reports for further information on how to use predefined database entitlement reports. To see entitlement reports, log on the user portal, and go to the DB Entitlements tab.

Note: DB Entitlements Reports are optional components enabled by product key. If these components have not been enabled, the choices do not appear in the Custom Domain Builder/Custom Query-Report Builder/Custom Table Builder selections.

The predefined entitlement reports are listed as follows. They appear as domain names in the Custom Domain Builder/Custom Query-Report Builder/ Custom Table Builder selections.

- Oracle DB Entitlements
- MYSQL DB Entitlements
- DB2® DB Entitlements
- SYBASE DB Entitlements
- Informix® DB Entitlements
- Microsoft SQL Server DB Entitlements
- Netezza® DB Entitlements
- Teradata DB Entitlements
- PostgreSQL DB Entitlements

## Oracle DB Entitlements

The following domains are provided to facilitate uploading and reporting on Oracle DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder/Custom Query-Report Builder/ Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports. To see entitlement reports, log on the user portal, and go to the DB Entitlements tab.

#### Oracle

- ORA Accnts of ALTER SYSTEM - Accounts with ALTER SYSTEM and ALTER SESSION privileges
- ORA Accnts with BECOME USER - Accounts with BECOME USER privileges
- ORA All Sys Priv and admin opt - Report showing all system privilege and admin option for users and roles
- ORA Obj And Columns Priv - Object and columns privileges granted (with or without grant option)
- ORA Object Access By PUBLIC - Object access by PUBLIC
- ORA Object privileges - Object privileges by database account not in the SYS and not a DBA role
- ORA PUBLIC Exec Priv On SYS Proc - Execute privilege on SYS PL/SQL procedures assigned to PUBL
- ORA Roles Granted - Roles granted to users and roles
- ORA Sys Priv Granted - Hierarchical report showing system privilege granted to users including recursive definitions (i.e. privileges assigned to roles and then these roles assigned to users)
- ORA SYSDBA and SYSOPER Accnts - Accounts with SYSDBA and SYSOPER privileges

For entitlements to be able to upload data from various datasources, the general requirement is that the login, used to access the database, be able to read the tables used in the query (which is hidden for all entitlements).

The following list (with comment line heading) details the minimal privileges required, in the database table (or view of the database table), in order for the entitlement to work.

```
/* Select privilege to these tables/views is required */

grant select on sys.dba_tab_privs to sqlguard;

grant select on sys.dba_roles to sqlguard;

grant select on sys.dba_users to sqlguard;

grant select on sys.dba_role_privs to sqlguard;

grant select on sys.dba_sys_privs to sqlguard;

grant select on sys.obj$ to sqlguard;

grant select on sys.user$ to sqlguard;

grant select on sys.objauth$ to sqlguard;

grant select on sys.table_privilege_map to sqlguard;

grant select on sys.dba_objects to sqlguard;

grant select on sys.v_$pwfile_users to sqlguard;

grant select on sys.dba_col_privs to sqlguard;
```

## MYSQL DB Entitlements

---

The following domains are provided to facilitate uploading and reporting on MYSQL DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder/Custom Query-Report Builder/ Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports. To see entitlement reports, log on the user portal, and go to the DB Entitlements tab.

MYSQL: The queries ending in \_40 use the most basic version of the mysql schema (for MySQL 4.0 and beyond). The information\_schema has not changed since it was introduced in MySQL 5.0, so there is a set of \_50 queries, but no \_51 queries. The \_50 queries work for MySQL 5.0 and 5.1 and for 6.0 when it comes out, since the information\_schema is not expected to change in 6.0. The queries ending in \_502 (MYSQL502) use the new information\_schema, which contains much more information and is much more like a true data dictionary.

- MYSQL Database Privileges 40
- MYSQL User Privileges 40
- MYSQL Host Privileges 40
- MYSQL Table Privileges 40
- MYSQL Database Privileges 500
- MYSQL User Privileges 500
- MYSQL Host Privileges 500
- MYSQL Table Privileges 500
- MYSQL Database Privileges 502
- MYSQL User Privileges 502
- MYSQL Host Privileges 502
- MYSQL Table Privileges 502

For entitlements to be able to upload data from various datasources, the general requirement is that the login, used to access the database, be able to read the tables used in the query (which is hidden for all entitlements).

The following list details the minimal privileges required, in the database table (or view of the database table), in order for the entitlement to work.

Note: In addition to the privileges required, the user should connect to the MYSQL database to upload the data.

The entitlement queries for all MySQL versions through MySQL 5.0.1 use this set of tables: mysql.db mysql.host mysql.tables\_priv mysql.user

Beginning with MySQL 5.0.2, and for all later versions, the entitlement queries use this set of tables: information\_schema.SCHEMA\_PRIVILEGES mysql.host information\_schema.TABLE\_PRIVILEGES information\_schema.USER\_PRIVILEGES

If a datasource has a MYSQL database type, but does not have a DB name (see Datasource Definitions, the database name under Location is blank), then the uploading data will loop through all MYSQL databases the user has access to.

## DB2 DB Entitlements

---

The following domains are provided to facilitate uploading and reporting on DB2 DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder/Custom Query-Report Builder/ Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports. To see entitlement reports, log on the user portal, and go to the DB Entitlements tab.

- DB2 Column-level Privileges (SELECT, UPDATE, ETC.)
- DB2 Database -level Privileges (CONNECT, CREATE, ETC.)
- DB2 Index-level Privilege (CONTROL)
- DB2 Package-level Privileges (on code packages – BIND, EXECUTE, ETC.)
- DB2 Table-level Privileges (SELECT, UPDATE, ETC.) DB2 Privilege Summary

For entitlements to be able to upload data from various datasources, the general requirement is that the login, used to access the database, be able to read the tables used in the query (which is hidden for all entitlements).

The following list (with comment line heading) details the minimal privileges required, in the database table (or view of the database table), in order for the entitlement to work.

```
/* Select privilege to these tables/views is required */
GRANT SELECT ON SYSCAT.COLAUTH TO SQLGUARD;
GRANT SELECT ON SYSCAT.DBAUTH TO SQLGUARD;
GRANT SELECT ON SYSCAT.INDEXAUTH TO SQLGUARD;
GRANT SELECT ON SYSCAT.PACKAGEAUTH TO SQLGUARD;
GRANT SELECT ON SYSCAT.DBAUTH TO SQLGUARD;
GRANT SELECT ON SYSCAT.TABAUTH TO SQLGUARD;
GRANT SELECT ON SYSCAT.SCHEMAAUTH TO SQLGUARD;
GRANT SELECT ON SYSCAT.PASSTHROUAUTH TO SQLGUARD;
```

## SYBASE DB Entitlements

---

The following domains are provided to facilitate uploading and reporting on SYBASE DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder/Custom Query-Report Builder/ Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports. To see entitlement reports, log on the user portal, and go to the DB Entitlements tab.

- SYBASE System Privilege and Roles Granted to User including Grant option
- SYBASE Role Granted to User and System Privileges Granted to user and role including Grant option
- SYBASE Object Access by Public
- SYBASE Execute Privilege on Procedure, function assigned To Public
- SYBASE Accounts with System or Security Admin Roles
- SYBASE Object and Columns Privilege Granted with Grant option
- SYBASE Role Granted To User

For entitlements to be able to upload data from various datasources, the general requirement is that the login, used to access the database, be able to read the tables used in the query (which is hidden for all entitlements).

The following list (with comment line heading) details the minimal privileges required, in the database table (or view of the database table), in order for the entitlement to work.

```
/* Select privilege to these tables/views is required */
/* These are required on MASTER database */
grant select on master.dbo.sysloginroles to sqlguard
grant select on master.dbo.syslogins to sqlguard
grant select on master.dbo.syssrvroles to sqlguard

/*These are required on every database, including MASTER */
grant select on sysprotects to sqlguard
grant select on sysusers to sqlguard
grant select on sysobjects to sqlguard
grant select on sysroles to sqlguard
```

If a datasource has a SYBASE database type, but does not have a DB name (see Datasource Definitions, the database name under Location is blank), then the uploading data will loop through all SYBASE databases the user has access to.

## Informix DB Entitlements

---

The following domains are provided to facilitate uploading and reporting on Informix DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder/Custom Query-Report Builder/ Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports. To see entitlement reports, log on the user portal, and go to the DB Entitlements tab.

- Informix Object Privileges by database account not including system account and roles
- Informix database level privileges, roles and language granted to user including grant option
- Informix database level privileges, roles and language granted to user and role including grant option
- Informix Object Grant to Public
- Informix Execute Privilege on Informix procedure and function granted to Public
- Informix Account with DBA Privilege Informix Object and columns privileges granted with Grant option
- Informix Role Granted To User and Role

For entitlements to be able to upload data from various datasources, the general requirement is that the login, used to access the database, be able to read the tables used in the query (which is hidden for all entitlements). The following list (with comment line heading) details the minimal privileges required, in the database table (or view of the database table), in order for the entitlement to work.

```
/* Select privilege to these tables/views is required */
```

Since all users have sufficient privileges for system catalog SELECT privileges, there is no need to grant privilege to any user. Informix doesn't seem to like granting system catalog to users. The grant would normally be used. But in this case they are not required.

```
grant select on systables to sqlguard;
grant select on systabauth to sqlguard;
grant select on sysusers to sqlguard;
grant select on sysroleauth to sqlguard;
grant select on syslangauth to sqlguard;
grant select on sysroutinelangs to sqlguard;
grant select on sysprocauth to sqlguard;
grant select on sysprocedures to sqlguard;
grant select on syscolauth to sqlguard;
```

If a datasource has a Informix database type, but does not have a DB name (see Datasource Definitions, the database name under Location is blank), then the uploading data will loop through all Informix databases the user has access to.

## Microsoft SQL Server 2005 and later DB Entitlements

---

The following domains are provided to facilitate uploading and reporting on Microsoft SQL Server 2005 and later DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder, Custom Query-Report Builder, and Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports. To see entitlement reports, log on the user portal, and go to the **DB Entitlements** tab.

Note: Objects in Dynamic query Strings will NOT be shown in xxx\_DEPENDENCIES. An object in an EXECUTE IMMEDIATE SQL string called by a stored program unit does not show dependency. This query exclude schema owner defined in group ID 202 "Dependencies\_exclude\_schema-MSSQL". User has the ability to add or subtract schema name from this group for the dependencies query.

- Microsoft SQL Server Object privileges by database account not including default system user.
- Microsoft SQL Server Role/System privileges granted To User
- Microsoft SQL Server Role/System Privilege granted to user and role including grant option
- Microsoft SQL Server Object access by PUBLIC
- Microsoft SQL Server Execute Privilege on System Procedures and functions to PUBLIC
- Microsoft SQL Server Database accounts of db\_owner and db\_securityadmin Role
- Microsoft SQL Server Server account of sysadmin, serveradmin and security admin /\* only run against MASTER database \*/
- Microsoft SQL Server Object and columns privileges granted with grant option
- Microsoft SQL Server Role granted to user and role.

For entitlements to be able to upload data from various datasources, the general requirement is that the login, used to access the database, be able to read the tables used in the query (which is hidden for all entitlements).

The following list (with comment line heading) details the minimal privileges required, in the database table (or view of the database table), in order for the entitlement to work.

```
/* Select privilege to these tables/views is required */
```

```
/*These are required on MASTER database */
```

```
grant select on sys.server_principals to sqlguard
```

```

/*These are required on every databases including MASTER */
grant select on sys.database_permissions to sqlguard
grant select on sys.database_principals to sqlguard
grant select on sys.all_objects to sqlguard
grant select on sys.database_role_members to sqlguard
grant select on sys.columns to sqlguard

```

If a datasource has a MSSQL database type, but does not have a DB name (see Datasource Definitions, the database name under Location is blank), then the uploading data will loop through all MSSQL databases the user has access to.

## Netezza DB Entitlements

---

The following domains are provided to facilitate uploading and reporting on Netezza DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder/Custom Domain Query/ Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports. To see entitlement reports, log on the user portal, and go to the **DB Entitlements** tab.

Note: There is no DB error text translation for Netezza. The error appears in the exception description. Users can clone/add a report with the exception description for Netezza as needed.

- Netezza Obj Privs by DB Username - Object privileges with or without grant option by database username excluding ADMIN account.
- Netezza Admin Privs by DB Username - Admin privileges with or without grant option by database username excluding ADMIN account.
- Netezza Group /Role Granted To User - Group (Role) granted to user
- Netezza Obj Privs By Group - Object privileges with or without grant option by GROUP excluding PUBLIC.
- Netezza Admin Privs By Group - Admin privileges with or without grant option by GROUP excluding PUBLIC.
- Netezza Admin Privs By DB Username, Group - Admin privileges with or without grant option by database username, group excluding ADMIN account and PUBLIC group.
- Netezza Obj Privs Granted - Object privileges granted with or without grant option to PUBLIC.
- Netezza Admin Privs Granted - Admin privileges granted with or without grant option to PUBLIC.
- Netezza Global Admin Priv To Users and Groups - Global admin privilege granted to users and groups excluding ADMIN account.
- Netezza Global Obj Priv To Users and Groups - Global object privilege granted to users and groups excluding ADMIN account.

For entitlements to be able to upload data from various datasources, the general requirement is that the login, used to access the database, be able to read the tables used in the query (which is hidden for all entitlements).

The following list (with comment line heading) details the minimal privileges required, in the database table (or view of the database table), in order for the entitlement to work.

```

/* Select privilege to these tables/views is required */

/* This script must be run from the system database */

GRANT SELECT ON SYSTEM VIEW TO sqlguard;

GRANT LIST ON DATABASE TO sqlguard;

GRANT LIST ON USER TO sqlguard;

GRANT LIST ON GROUP TO sqlguard;

GRANT SELECT ON _V_CONNECTION TO sqlguard;

```

For Netezza entitlement queries, it is recommended to connect to SYSTEM database, especially when granting the privilege to the user who is going to run these reports. The granting privilege MUST take place from SYSTEM database or else the granted privilege will only take place on one particular database. When the granted privilege takes place from SYSTEM database, a special feature will allow the granted privilege to carry through to all the databases.

## Teradata DB Entitlements

---

The following domains are provided to facilitate uploading and reporting on Teradata DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder/Custom Domain Query/ Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports. To see entitlement reports, log on the user portal, and go to the **DB Entitlements** tab.

- Teradata Object privileges by database account not including default system users.
- Teradata System privileges and roles granted to users including grant option.
- Teradata Roles granted to users and roles including grant option.
- Teradata Role granted to users and roles. System privileges granted to users and roles including grant option.

- Teradata Objects and System privileges granted to public. Note role cannot be granted to public in Teradata.
- Teradata Execute privileges on system database objects to public.
- Teradata System admin, Security admin privileges granted to user and role.  
Note: There are no such role as System or Security admin in Teradata. User must create their own roles. These are some important system privileges that would normally not be granted to normal user: ABORT SESSION, CREATE DATABASE, CREATE PROFILE, CREATE ROLE,CREATE USER, DROP DATABASE, DROP PROFILE, DROP ROLE, DROP USER, MONITOR RESOURCE, MONITOR SESSION, REPLICATION OVERRIDE, SET SESSION RATE, SET RESOURCE RATE.
- Teradata Object privileges granted with granted option to users. Not including DBC and grantee = 'All'.

For entitlements to be able to upload data from various datasources, the general requirement is that the login, used to access the database, be able to read the tables used in the query (which is hidden for all entitlements).

The following list (with comment line heading) details the minimal privileges required, in the database table (or view of the database table), in order for the entitlement to work.

```
/* Select privilege to these tables/views is required */

GRANT SELECT ON DBC.AllRights TO sqlguard;

GRANT SELECT ON DBC.Tables TO sqlguard;

GRANT SELECT ON DBC.AllRoleRights TO sqlguard;

GRANT SELECT ON DBC.RoleMembers TO sqlguard;
```

## PostgreSQL DB Entitlements

---

The following domains are provided to facilitate uploading and reporting on PostgreSQL DB Entitlements. Each of the following domains has a single entity (with the same name), and there is a predefined report for each domain. All of these domains are available from the Custom Domain Builder/Custom Domain Query/ Custom Table Builder selections. As with other predefined entities and reports, these cannot be modified, but you can clone and then customize your own versions of any of these domains or reports. To see entitlement reports, log on the user portal, and go to the **DB Entitlements** tab.

There are seven entitlement custom domains/queries/reports for PostgreSQL. They are as follows (each is listed with Report name, description, note):

- PostgreSQL Priv On Databases Granted To Public User Role With Or Without Granted Option. Privilege on databases granted to public, user and role with or without granted option. Run this on any database, ideally PostgreSQL.
- PostgreSQL Priv On Language Granted To Public User Role With Or Without Granted Option. Privilege on Language granted to public, user and role with or without granted option. Run this per database.
- PostgreSQL Priv On Schema Granted To Public User Role With Or Without Granted Option. Privilege on Schema granted to public, user and role with or without granted option. Run this per database.
- PostgreSQL Priv On Tablespace Granted To Public User Role With Or Without Granted Option. Privilege on Tablespace granted to public, user and role with or without granted option. Run this on any database, ideally PostgreSQL.
- PostgreSQL Role Or User Granted To User Or Role. Role or User granted to user or role including grant option. Run this once in any database. Ideally PostgreSQL.
- PostgreSQL Super User Granted To User Or Role. Super user granted to user or role. Run this once in any database. Ideally PostgreSQL.
- PostgreSQL Sys Prvs Granted To User And Role. System privileges granted to user and role. Run this once in any database. Ideally PostgreSQL.
- PostgreSQL Table View Sequence and Function prvs Granted To Public. Tables, Views, Sequence and Functions privileges granted to public. Run this per database. Run this per database.
- PostgreSQL Table View Sequence and Function Prvs Granted With Grant Option. Tables, Views, Sequence and Functions privileges granted to user and role with grant option only. Exclude PostgreSQL account.
- PostgreSQL Table View Sequence Function Prvs Granted To Roles. Tables, Views, Sequence and Functions privileges granted to roles. Not including public. Run this per database.
- PostgreSQL Table Views Sequence and Functions Prvs Granted To Login. Tables, Views, Sequence and Functions privileges granted to logins. Not including postgres system user. Run this per database.

Note: As of version 8.3.6, PostgreSQL does not support grant admin option to public. There is only function, no store procedure. There is no support for column grant, only table grant. Public is a group, not user. Public does not show up in pg\_roles. The only privileges need to run all these queries is: GRANT CONNECT ON DATABASE PostgreSQL TO username;

For entitlements to be able to upload data from various datasources, the general requirement is that the login, used to access the database, be able to read the tables used in the query (which is hidden for all entitlements).

The following list (with comment line heading) details the minimal privileges required, in the database table (or view of the database table), in order for the entitlement to work.

```
/* Select privilege to these tables/views is required */

/*This is required on POSTGRES database*/
```

```

grant connect on database postgres to sqlguard;

/*These are required on every database, including POSTGRES (By default these are already granted to PUBLIC) */

grant select on pg_class to sqlguard;
grant select on pg_namespace to sqlguard;
grant select on pg_roles to sqlguard;
grant select on pg_proc to sqlguard;
grant select on pg_auth_members to sqlguard;
grant select on pg_language to sqlguard;
grant select on pg_tablespace to sqlguard;
grant select on pg_database to sqlguard;

```

If a datasource has a PostgreSQL database type, but does not have a DB name (see Datasource Definitions, the database name under Location is blank), then the uploading data will loop through all PostgreSQL databases the user has access to.

## Data Mart

Use data marts to extract data for subsequent use. Use datamarts for more efficient storage of frequently accessed data; for data that you want to preserve after its purge time; for exporting data from Guardium; and for creating distributed reports.

The Data Mart extraction program runs in a batch according to the specified schedule. It summarizes the data to hours, days, weeks, or months according to the granularity requested and then it saves the results in the Guardium Datamart database. The data is accessible to the users via the standard Reports and Audit Process utilities, like any other domain/entity. The Data Mart extraction data is available under the DM domain. The Entity name is set according to the new table name specified for the data mart data. Using the standard Query-Report Builder, you can clone the query and edit the Query-Report.

The summarization of data shrinks the data volume significantly. It eliminates joins of many tables by storing the data analysis in un-normalized and pre-calculated tables.

There are two types of data marts:

- Extract data to table (in Guardium).
- Extract data to file, for exporting to an external system.

### Central Management and Data Mart

In a Central Management environment, the configuration is distributed automatically to the managed units. The extraction schedule is defined locally on each unit. In case of multiple Central Managers, the Data Mart definition can be cloned by using the Export/Import capability.

- [Viewing your data marts](#)  
The Data marts page is a handy reference for all the data marts defined in your system. You can filter by type, or free search, and you can view the related queries, the extraction log, and view the data mart configuration.
- [Extracting data mart to table](#)  
Use data mart tables, for example, for frequently accessed data, systems with large-scale data that you want available for reports, and data you want to preserve after the scheduled purge. Data marts improve the performance of online reports on Guardium® aggregators.
- [Extracting data mart to file](#)  
You can create your own data mart extractions to CSV file, for export to a destination host.
- [Manage predefined data extraction to file](#)  
Guardium has pre-defined data extractions to file that are disabled by default. You can enable the export extractions by scheduling them through GuardAPI commands.

## Viewing your data marts

The Data marts page is a handy reference for all the data marts defined in your system. You can filter by type, or free search, and you can view the related queries, the extraction log, and view the data mart configuration.

## Procedure

1. Go to Reports > Report Configuration Tools > Data Marts.
2. To filter the data marts, select a domain from the drop-down list, or click either the File or Table radio buttons, or type text in the Filter field.
3. To view the query associated with a data mart, select the data mart, and click Action > Open related query.
4. To view the extraction log for a data mart, select the data mart, and click Action > Open data mart extraction log.
5. To view the data mart configuration, select the data mart, and click Action > Open data mart config.
6. To view and manage the data mart queries, select the data mart, and click Action > List data mart queries. This action is available only for the data marts with type Table.

## Extracting data mart to table

Use data mart tables, for example, for frequently accessed data, systems with large-scale data that you want available for reports, and data you want to preserve after the scheduled purge. Data marts improve the performance of online reports on Guardium® aggregators.

## Before you begin

---

Prerequisite: Data Mart Builder access rights (User Role).

## About this task

---

There are no predefined data marts of the table type. You can create data mart tables from reports that have the data mart icon . The data mart summarizes the data by hours, days, weeks, or months according to the granularity you specify. When you create a table data mart, Guardium creates a query-report with the name you assigned. You can modify this query-report just as you modify any other query-report. You can copy the query-report and modify it to suit your exact needs. Guardium also creates a custom domain and a custom table of the same name. [External data correlation](#) describes using custom domains and custom tables.

You can use the parameters in these reports to run functions (API) to generate scripts. See [Working with API calls and reports](#).

**Data Mart persistency:** Changes to the original query or report do not affect the Data Mart; a snapshot of the originated analysis definition is saved together with the Data Mart upon creation.

When a data mart extraction runs (Scheduled or Run once now) for the first time, it extracts data from Initial start date to the current time based on the Time granularity. It saves the next period from in the DM\_EXTRACTION\_STATE table. On the next run, it extracts data starting from the next period from.

The extracted file name is <Global Id>\_<short host name of source machine>\_<file name defined by user>\_<period start date time short format in UTC>.gz; for example: 1762144738\_gibm32\_LOGS\_20181028230000\_COMPLETE.gz

You can track the extraction and see the overall datamart status in the pre-defined Datamart Extraction Log report. View the User Defined Extraction Log for details on user-defined extractions, for example, datamarts and distributed reports.

To see a list of all data marts to which you have access, navigate to: Reports > Report Configuration Tools > Data Mart. From that page, you can open and modify the data marts.

After a data mart is created, you can modify its Purge After days, its archive schedule, and its schedule. To access the data mart, access the report from which you created the data mart, click , select the data mart from the list of data marts based on this report, and use the instructions in this procedure. If you have a data mart selected, and you want to create a new data mart, click New.

## Procedure

---

1. Access the report you want to create a data mart from and click . The Data Mart dialog opens.
2. Enter a Data Mart name. Optionally, enter a description.
3. In the Extract result to row, verify that Table is selected.
4. Optionally, enter a Table Name. If not specified, it is saved as DM. It's helpful to define an intuitive name, since you can define indexes in the Custom Domain, and check table sizes using the GuardAPI.
5. Specify a time granularity. This is the granularity of the resulting data mart table. Match your granularity to the frequency at which you'll run the corresponding reports: hourly, daily, monthly.
6. The Archive/Export option controls whether the data from this data mart table is included in the data export and data archive, if these processes are configured on this unit. Select Yes if you want to enable data export and data archive for this data mart.
7. Set the number of purge days. The purge days should reflect your business case, for example, the number of days you need that data for your reports, the size of data, available disk space.
8. Select an initial start time from the calendar icon. This is the date/time from which you want the data extracted when the data mart extraction runs for the first time. For example, you define the data mart on Nov 5, 2018, but you need data from Nov 1, 2018. In this case, set Initial Start to Nov 1, 2018.
9. Click Apply to save the Data Mart.
10. To define data extraction on a regular basis, in the scheduling section click Modify Schedule, then define the data mart extraction schedule.
  - Start time: time of day the extraction starts
  - Restart: leave at Run only once
  - Schedule by: select Day/Week
  - Click Every day
  - Schedule Start Time: leave blank unless you want to start the datamart in the future. In that case, open the calendar and select the date on which to start exporting the data mart.
  - Automatically run dependent jobs. Leave unchecked. It is not relevant for data mart.
11. Select the user roles that have access to this datamart:
  - a. Click Roles.
  - b. In the Roles dialog, either select All Roles, or the individual roles.
  - c. Click Apply. The roles are saved and the dialog closes.
12. To temporarily stop report extraction click Pause, click Resume to resume report extraction.
13. To run the extraction once in real time, click Run Once Now.

## Related reference

---

- [Data mart APIs](#)

## Extracting data mart to file

---

You can create your own data mart extractions to CSV file, for export to a destination host.

## About this task

---

The names of extracted CSV files have the format <filename defined by user>\_<period start date time short format>.csv. For example, EXP\_SESSION\_LIST\_20180219060000.csv. They are stored in the location you specify when you define the extraction. After you define an extract to file, you can use all the GuardAPI commands on those extracts.

Data mart file names must follow Linux rules. For example, the file name can't include \$ because Linux does not support it. If you create a file with the name `my$file`, the saved file name is `my`.

Data mart file names must follow Linux rules for naming files. For example, file names can't include "\$' since Linux doesn't support it. If you try to create a file named `my$file`, the saved file name is `my`.

You can track the extraction and see the overall data mart status in the pre-defined Datamart Extraction Log report.

The data mart configuration commands are run only once per central manager, since all collectors can then receive this information from the central manager.

**Bundled data marts:** You can bundle a number of CSV export data marts together, both user-defined and pre-defined. Each bundle has a main data mart. Each data mart that is included in a bundle pulls out data based on its own scheduling. After the main data mart extracts data, it puts data files from all the data marts included in the bundle into the one tar file, and sends it to a destination server. The main data mart must have the latest scheduled extraction time of all the data marts in the bundle so that it can include all the other data marts' latest extracts. See [datamart copy file bundle](#).

If you are defining the export by API, you need to know which unit types are relevant for the various domains. Some guidelines for commonly used domains:

- Classification, discovered instances, outliers, vulnerability assessment: on the units where these processes are enabled or scheduled.
- Exceptions, groups, system information, unit utilization levels: all units.
- Access, policy violations, S-TAP status: collectors only.
- Datasources, users: central manager, standalone.

## Procedure

---

1. Access the report you want to create a data mart from and click . The Data Mart dialog opens.
2. In the Data Mart Configuration section, enter a Data Mart Name. The data mart name must start with **Export**:
3. Optional: Enter a Description.
4. In the Extract result to row, select File.
5. Enter a File Name. The file name must start with `EXP_`
6. Optional: Enter a File Path. If left blank, files are saved in: /opt/IBM/Guardium/data/dump/DATAMART/. The group `guarddatamart` or the group `guardaggpids` must have write access to the file location. The location must have all permissions for mysql and tomcat users; and is accessible from the file server. For example,
  - /var/IBM/Guardium/TSM/
  - /var/IBM/Guardium/data/exportdir/
7. Specify a Time Granularity for the resulting data mart table. Match your granularity to the frequency at which you run the corresponding reports: hourly, daily, monthly.
8. Select an Initial Start time from the calendar icon, indicating the date and time for the start of the data extraction. For example, you define the data mart on November 5, 2018, but you need data from November 1, 2018. In this case, set Initial Start to November 1, 2018.
9. Click Apply to save the Data Mart.
10. To define a regular data extraction, in the scheduling section click Modify Schedule. Define the data mart extraction schedule.
  - Start time: time of day the extraction starts
  - Restart: leave at Run only once
  - Schedule by: select Day/Week
  - Click Every day
  - Schedule Start Time: leave blank unless you want to start the data mart in the future. In that case, open the calendar and select the date on which to start exporting the data mart.
  - Automatically run dependent jobs. Leave cleared. It is not relevant for data mart.
11. Select the user roles that have access to this data mart:
  - a. Click Roles.
  - b. In the Roles dialog, either select All Roles, or the individual roles.
  - c. Click Apply. The roles are saved and the dialog closes.
12. To temporarily stop report extraction click Pause, click Resume to resume report extraction.

## Related reference

---

- [Data mart APIs](#)

## Manage predefined data extraction to file

---

Guardium has pre-defined data extractions to file that are disabled by default. You can enable the export extractions by scheduling them through GuardAPI commands.

## About this task

---

The predefined extractions to file are listed in [Table 1](#). By default, extractions are hourly. You can modify the frequency, however, there are suggested execution times for the pre-defined extractions, based on internal Guardium processes. They are presented in [Table 2](#).

The format of the extracted file name is <Global Id>\_<short host name of source machine>\_<export job name>\_<period start date time short format in UTC>.gz, for example: 1762144738\_machine1\_EXP\_SESSION\_LOG\_20181028230000.gz

If a file transfer fails for any reason, for example if the target machine is down, then it retries the transfer on the next run. The backlog is kept in /var/exportdir directory, and the backlog purge interval is twice the data extraction log purge interval. Use the CLI command `show purge objects age` to view purge intervals. Set the datamart

extraction log purge interval using the CLI command store **purge object age 31 [age]** where [age] is the desired purge interval.

Full\_SQL data mart only works if log full details or log masked details is defined and installed.

Outlier data mart only works if outlier detection is enabled.

If data mart/s scheduler had been stopped for some time and you don't want the data to be extracted retroactively, then before you reschedule extractions to run again, set the correct "Initial Start" in the Data Mart Configuration screen.

Table 1. Predefined data mart export jobs

| Datamart Name / job description / objectName | Description                                                                                                                                                                                                                                                             | Report Title                                 | Unit Type                   | Datamart ID | jobname                   |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------|-------------|---------------------------|
| Export:Access Log                            | Includes details of the connection information and the activity summary per hour. The log includes the OS and DB user, successful and failed SQLs, client and server IP and more.                                                                                       | Export: Access Log                           | Collector                   | 22          | DataMartExtract ionJob_22 |
| Export:Session Log                           | Includes details about datasources' sessions (login to logout). The log includes session start and end timestamps, OS and DB user of the session, source program and more.                                                                                              | Export: Session Log                          | Collector                   | 23          | DataMartExtract ionJob_23 |
| Export:Session Log Ended                     | Session may extend for long period. The extraction works hourly. This log sends the sessions that ended later than the hour started.                                                                                                                                    | Export: Session Log                          | Collector                   | 24          | DataMartExtract ionJob_24 |
| Export:Exception Log                         | Details the Exceptions / Errors captured by Guardium. The log will includes exception/error description, user name, source address, DB protocol and more.                                                                                                               | Export: Exception Log                        | Any                         | 25          | DataMartExtract ionJob_25 |
| Export:Full SQL                              | Includes the executed SQL details. The log includes full SQL, records affected, session ID and more.                                                                                                                                                                    | Export: Full SQL                             | Collector                   | 26          | DataMartExtract ionJob_26 |
| Export:Outliers List                         | Includes the outliers. The log includes server IP, DB user, Outlier type, DB and more.                                                                                                                                                                                  | Analytic Outliers List                       | Any                         | 27          | DataMartExtract ionJob_27 |
| Export:Outliers Summary by hour              | Includes an hour summary of outliers. The log includes server IP, DB user, DB and more.                                                                                                                                                                                 | Analytic Outliers Summary                    | Any                         | 28          | DataMartExtract ionJob_28 |
| Export:Group Members                         | Includes a log of all groups members. The log includes Group type, Group description, Group member and Tuple Flag.                                                                                                                                                      | Export:Group Members                         | Any                         | 29          | DataMartExtract ionJob_29 |
| Export:Export Extraction Log                 | Includes log of data relevant to all export or copy files having a name starting with "Export:"                                                                                                                                                                         | User Defined Extraction Log                  | Any                         | 31          | DataMartExtract ionJob_31 |
| Export:Policy Violations                     | Includes the details about logged violations, such as DB User, Source Program, Access Rule Description, Full SQL String and more.                                                                                                                                       | Export:Policy Violations                     | Collector                   | 32          | DataMartExtract ionJob_32 |
| Export:Buff Usage Monitor                    | Provides an extensive set of sniffer buffer usage statistics                                                                                                                                                                                                            | Buff Usage Monitor                           | Any                         | 33          | DataMartExtract ionJob_33 |
| Export:VA Results                            |                                                                                                                                                                                                                                                                         | Security Assessment Export                   | Any                         | 34          | DataMartExtract ionJob_34 |
| Export:Policy Violations - Detailed          | The same as Export Extraction Log, but has Object/Verb tuples. It is recommended that only one of them has to be used.                                                                                                                                                  | Export:Policy Violations                     | Collector                   | 38          | DataMartExtract ionJob_38 |
| Export:Access Log - Detailed                 | The same as Access Log, but also has the following fields from Application Event entity: Event User Name, Event Type, Event Value Str, Event Value Num, Event Date. It is recommended that Access Log or Access Log – Detailed should be used and not the both of them. | Export: Access Log                           | Collector                   | 39          | DataMartExtract ionJob_39 |
| Export:Discovered Instances                  | Provides the result of S-TAP Discovery application, which discovers database instances                                                                                                                                                                                  | Discovered Instances                         | Any                         | 40          | DataMartExtract ionJob_40 |
| Export:Databases Discovered                  |                                                                                                                                                                                                                                                                         | Databases Discovered                         | Any                         | 41          | DataMartExtract ionJob_41 |
| Export:Classifier Results                    |                                                                                                                                                                                                                                                                         | Classifier Results                           | Any                         | 42          | DataMartExtract ionJob_42 |
| Export:Datasources                           |                                                                                                                                                                                                                                                                         | Data-Sources                                 | Central Manager, Standalone | 43          | DataMartExtract ionJob_43 |
| Export:STAP Status                           |                                                                                                                                                                                                                                                                         | S-TAP Status Monitor                         | Collector                   | 44          | DataMartExtract ionJob_44 |
| Export:Installed Patches                     |                                                                                                                                                                                                                                                                         | Installed Patches                            | Any                         | 45          | DataMartExtract ionJob_45 |
| Export:System Info                           |                                                                                                                                                                                                                                                                         | Installed Patches                            | Any                         | 46          | DataMartExtract ionJob_46 |
| Export:User - Role                           |                                                                                                                                                                                                                                                                         | User - Role                                  | Central Manager, Standalone | 47          | DataMartExtract ionJob_47 |
| Export:Classification Process Log            |                                                                                                                                                                                                                                                                         | Classification Process Log                   | Any                         | 48          | DataMartExtract ionJob_48 |
| Export:Outliers List - enhanced              |                                                                                                                                                                                                                                                                         | Analytic Outliers List - enhanced            | Any                         | 49          | DataMartExtract ionJob_49 |
| Export:Outliers Summary by hour - enhanced   |                                                                                                                                                                                                                                                                         | Analytic Outliers Summary by Date - enhanced | Any                         | 50          | DataMartExtract ionJob_50 |

Table 2. Default cronString for predefined data mart export jobs

| Job description                            | Recommended cronString        | Every hour at:  |
|--------------------------------------------|-------------------------------|-----------------|
| Export:Access Log                          | 0 40 0/1 ? * 1,2,3,4,5,6,7    | 00:40           |
| Export:Session Log                         | 0 45 0/1 ? * 1,2,3,4,5,6,7    | 00:45           |
| Export:Session Log Ended                   | 0 46 0/1 ? * 1,2,3,4,5,6,7    | 00:46           |
| Export:Exception Log                       | 0 25 0/1 ? * 1,2,3,4,5,6,7    | 00:25           |
| Export:Full SQL                            | 0 30 0/1 ? * 1,2,3,4,5,6,7    | 00:30           |
| Export:Outliers List                       | 0 10 0/1 ? * 1,2,3,4,5,6,7    | 00:10           |
| Export:Outliers Summary by hour            | 0 10 0/1 ? * 1,2,3,4,5,6,7    | 00:10           |
| Export:Export Extraction Log               | 0 50 0/1 ? * 1,2,3,4,5,6,7    | 00:50           |
| Export:Group Members                       | 0 15 0/1 ? * 1,2,3,4,5,6,7    | 00:15           |
| Export:Policy Violations                   | 0 5 0/1 ? * 1,2,3,4,5,6,7     | 00:05           |
| Export:Buff Usage Monitor                  | 0 12 0/1 ? * 1,2,3,4,5,6,7    | 00:12           |
| Export:VA Results                          | 0 0 2 ? * 1,2,3,4,5,6,7       | Daily at 2 AM   |
| Export:Policy Violations - Detailed        | 0 5 0/1 ? * 1,2,3,4,5,6,7     | 00:05           |
| Export:Access Log - Detailed               | 0 40 0/1 ? * 1,2,3,4,5,6,7    | 00:40           |
| Export:Discovered Instances                | 0 20 0/1? * 1,2,3,4,5,6,7     | 00:20           |
| Export:Databases Discovered                | 0 20 0/1? * 1,2,3,4,5,6,7     | 00:20           |
| Export:Classifier Results                  | 0 20 0/1? * 1,2,3,4,5,6,7     | 00:20           |
| Export:Datasources                         | 0 0 7 ? * 1,2,3,4,5,6,7       | Daily at 7 AM   |
| Export:STAP Status                         | 0 0/5 0 0/1 ? * 1,2,3,4,5,6,7 | Every 5 minutes |
| Export:Installed Patches                   | 0 0 5 ? * 1,2,3,4,5,6,7       | Daily at 5 AM   |
| Export:System Info                         | 0 0 5 ? * 1,2,3,4,5,6,7       | Daily at 5 AM   |
| Export:User - Role                         | 0 5 0/1 ? * 1,2,3,4,5,6,7     | 00:05           |
| Export:Classification Process Log          | 0 25 0/1 ? * 1,2,3,4,5,6,7    | 00:25           |
| Export:Outliers List - enhanced            | 0 10 0/1 ? * 1,2,3,4,5,6,7    | 00:10           |
| Export:Outliers Summary by hour - enhanced | 0 10 0/1 ? * 1,2,3,4,5,6,7    | 00:10           |

## Procedure

---

1. Enable the appropriate datamarts and point their output to your target server, for example:

```
grdapic datamart_update_copy_file_info destinationHost=<destination server name>
destinationPassword=<destination server PW>
destinationPath=<destination server> destinationUser=<destination server user>
Name="Export:Session Log" transferMethod=SCP
```

2. Schedule the extraction. Guardium schedulers are local to the appliance, so you need to run the GuardAPI scheduling command on each appliance from which data is extracted. For example, for each collector that needs to send session data you would run:

```
grdapic schedule_job jobType=dataMartExtraction cronString=0 45 0/1 ? * 1,2,3,4,5,6,7
objectName="Export:Session Log"
```

## Related reference

---

- [Data mart APIs](#)

## Distributed Report Builder

---

This central manager feature provides a way to automatically gather data from all or a subset of the Guardium managed units that are associated with this particular central manager. Distributed reports are designed to provide a high-level view, to correlate data from across data sources, and to summarize views of the data. Continue to use aggregators for the row level data gathering across collectors.

This capability alleviates an issue that can arise in complex enterprise environments when users do not always know the exact managed unit that has the data that is required to for a particular report. This can happen because the link between Guardium collectors and databases can change over time, for example depending on configuration options such as load balancing. This is further complicated by considerations such as the time period and data retention policy on the aggregator and collectors.

It is easy to create a Distributed Report. Simply define it via the Distributed Report Configuration page, add to My Dashboard.

Distributed reports optionally make use of data marts on the central manager to enable scheduled collection of aggregated data over time. The distributed report data is stored as a flat table, so no complex joins are required to create the report you want. The report aggregates summarized and analyzed data from all units to enable a high-level/corporate view in a reasonable response time.

Distributed report data can be gathered from collectors, aggregators, and even central managers. The default distributed versions of the reports includes the host name of the unit responsible for that data.

There are two types of distributed reports:

- Immediate reports present a limited amount of data from each unit from its "gather data from" list. It does this on demand.
- Scheduled reports run in the background as defined by its schedule and time granularity and saves data in a table on primary and secondary, if defined, targets.

The following are predefined distributed reports:

- Enterprise S-TAP Verification
- Aggregation/Archive Log

- Failed User Login Attempts
- Scheduled Jobs Exceptions

Prerequisites – create group of Managed Units via the Central Management screen.

1. Create Distributed Report.
2. Review the data gathered.
3. Create additional summary reports on the data gathered.

Running Distributed reports: Immediate or scheduled

When you define a distributed report, run it immediately or schedule it to run in the background and gather the results to the Central Manager:

- **Immediate:** This mode gathers data on demand (upon execution via the GUI) and displays results while gathering the results from the relevant managed units. The distributed report includes a status indicator that data is still in transit or that all data has been received from a particular managed unit. In this mode, data is not saved on the Central Manager. As soon as the report is closed, the data is gone. Results for immediate reports are limited to 100 rows. Immediate reports have two export options: Download Display records and Download as PDF.
- **Scheduled:** This mode gathers data in advance in order to enable instant response. On the time interval you specify in the scheduler, all relevant, aggregated data from the specified managed units is sent to a designated data mart table on the Central Manager machine and creates a default report against this table. This table also has its own domain and entity to enable creation of additional queries and reports using the query builder. Those reports can be added to an audit process in order to run the process periodically and assign the results of the process to a Role, User and/or User Group for review or sign-off. Results for scheduled reports are limited to 10000 rows by default, but the limit is configurable using the **store scheduled\_distributed** CLI command. Scheduled reports have these export options: Download all records, Download display records, Full printable report, and Download as PDF.

Planning considerations for distributed reports

- In a mixed environment where the Central Manager is 32-bit and managed units are 64-bit, the Distributed Report will not show information from the 64-bit systems. To see information in this situation, the Central Manager needs to be upgraded to 64-bit.
- Because of the coordination of data to be sent to the Central Manager, it is critical that the clock time on all managed units is set to the real-time at the time zone where the managed units are located. Even a difference of ten minutes between the Central Manager and the managed units impact the performance and reliability of the distributed reports.
- Scheduled Distributed report definitions can be exported and imported, however immediate Distributed Report definitions cannot be exported or imported. The schedule itself is not included in the exported and imported definition. It is recommended that you keep a record of the definitions and scheduling if needed to re-create on another system such as a backup or test Central Manager. System backup does include distributed report configurations.
- If you specify that report data is collected from both aggregators and collectors, it is conceivable that the default distributed report includes duplicate data (although the Guardium host name is different). In this case, it is best to specify only collectors or only aggregators for the distributed report configuration.
- Distributed reports are based on existing non-distributed reports. When defining a distributed report in scheduled mode, if the original query includes run-time parameters, then you will be asked to provide those values (or wildcards, %).
- You can choose the target Guardium system for each scheduled distributed report. (By default, the target is the central manager. The list of available target systems is set by the GRDAPi command: **grdap set\_distributed\_report\_target target\_host\_name=[unit host name]**.) The target system will have data residing on its database that it did not have previous to the distributed report. Plan ahead for operational changes for purging, upgrades, and backup.

#### Edit and update

For distributed reports, edit and update the base report and update the distributed report based on the updated report structure.

If a user changes the columns in a base report, or adds or removes the where clause in the base report, and then saves and re-generates the report, then to update the distributed report based on this updated report, the user only needs to click on "Save report changes" on the existing distributed report for changes to take effect.

Should the user choose to update the existing report parameter, user should first click on "Apply report changes", then update the parameter value, then click on "Save report changes" for the updates to take effect.

#### More about time

When running a report, the report customizer lets you specify an absolute time window for the query (from 3-31-2014 8:00am to 3-31-2014 11:00am) or a relative time window (NOW -3 HOUR).

For absolute time, each Guardium system will run in its local time. For example, if a distributed report gathers data from Guardium systems in Eastern Standard Time (EST) and Pacific Standard Time (PST), then each system will execute the query based on local time. In the example (useful for checking morning peak hours, midnight or any specific absolute time), a system in New York will gather the results from 08:00 - 11:00 EST and a system in California will gather the results from 08:00 - 11:00 PST.

For a relative time specification, each system will run NOW -N according to the current time on that system. This is important for real-time reports. Absolute Time cannot be used for real-time or near real-time reports. Use the Immediate mode for real-time monitoring.

#### Viewing Distributed Report Status

Every distributed report is accompanied by a status report that shows the user what machines succeed in bringing in the results and what did not. The link to access the status report is highlighted when you navigate to the report in the GUI.

For scheduled reports, clicking on a line on the Status Report enables execution of API to rerun the report on the specific unit(s).

If the specific run for Distributed Report in Scheduled mode comes back with an error, you can rerun the report from the status report as follows:

1. Double click on one of the rows in the status report to bring up the Invoke menu. Click on Invoke.
2. Click the selection, rerun\_distributed\_report.
3. This will open up a pop-up screen that lets you choose the specific run to rerun. Any row of the report can be opened, but only rows with ERROR status can be rerun.

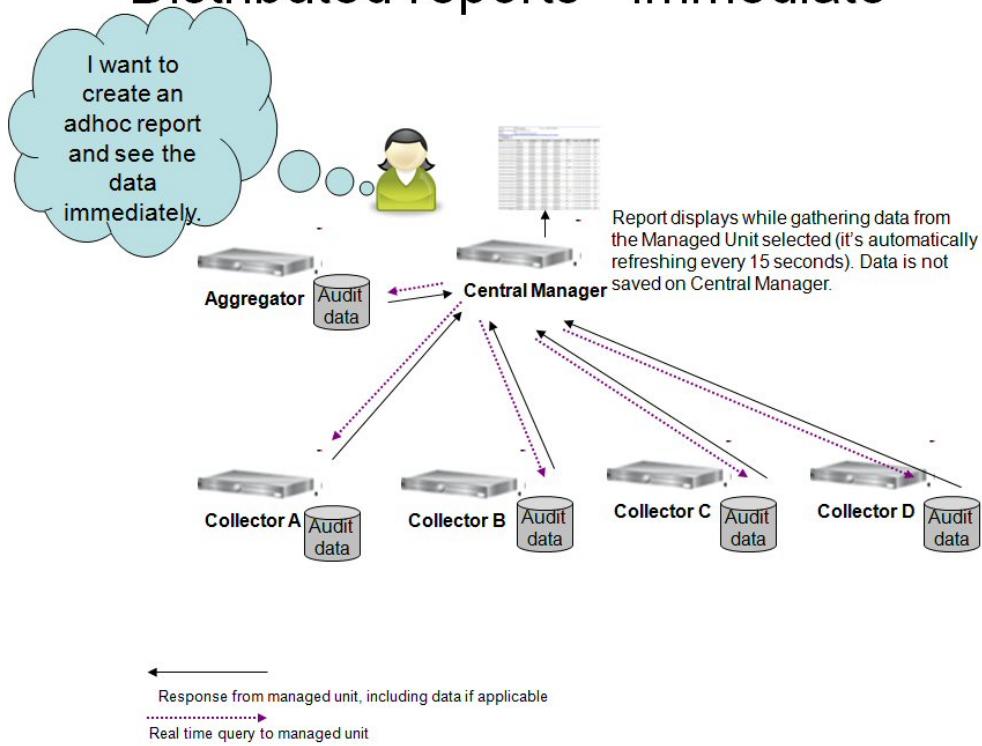
#### GuardAPI for Rerun Distributed Report

The retry command described in the GUI, for invoking the status report, can also be accessed via GuardAPI command.

#### Syntax

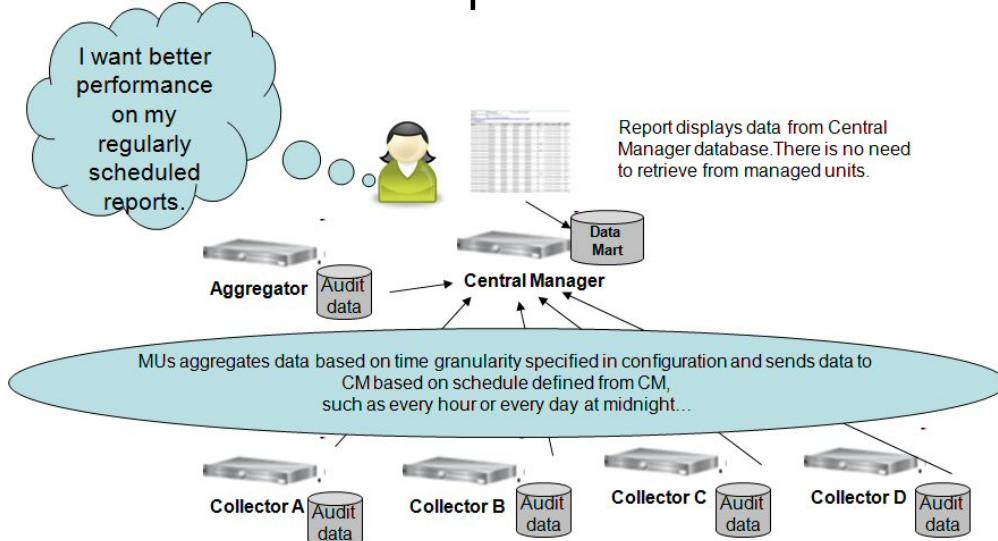
```
grdap rerun_distributed_report
```

# Distributed reports - Immediate



This diagram illustrates the process to run an Immediate Distributed Report.

# Distributed reports - scheduled



This diagram illustrates the process to schedule a Distributed Report.

Distributed Report enhancement - set Target system to any Guardium system

The Distributed Reports distributes the query request to the specified Guardium systems, it gathers the data into the Target system, consolidates the results and provides views on the consolidated results. The results are available via the Query Builder for additional queries definition.

The Distributed Report feature can now set the Target system to any Guardium system. The previous version does not allow setting the Target system and it always goes to the Central Manager (CM).

Requirement justification

In many cases the CM is overloaded (regardless of the Distributed Report) and the CM is sometime used as an Aggregator which adds load to the CM.

In those cases it will be much more efficient to enable the user to determine the target system.

Solution

- A target System can be set for each Distributed Report. A CLI command is available to set the optional Target systems. The list set via the CLI is shown in the Distributed Report builder GUI.
- Note: This change affects the Distributed Report Scheduled mode only. The Immediate mode is not included in this change! This means that the ad-hoc distributed report result viewer is accessible via the CM only.
- The Distributed Report definition is still editable via the CM only.

The CLI commands (available via the CM only)

1. Set System as a Target System

```
grdapic set_distributed_report_target target_host_name=[unit host name]
```

2. Cancel System to be a Target system

```
grdapic cancel_distributed_report_target target_host_name=[unit host name]
```

If there are still distributed reports with this unit as target then returns error and the list of such reports

3. Get list of Target systems

```
grdapic get_distributed_report_target_info
```

Additional CLI commands:

For scheduled distribute reports, store or show the value of a maximum number of rows per unit:

```
show scheduled_distributed
store scheduled_distributed
```

The **store** command has one parameter, maximum\_rows\_per\_unit. If the value of that parameter is greater than 15,000 or equals 0 (no limit), the following warning message displays:

Depending on number of collectors, setting maximum number of rows per unit to a high value might have negative impact on performance.

- [Creating a Distributed Report](#)

Create and modify distributed reports on a central manager.

## Related reference

- [Reports and report generation APIs](#)

## Creating a Distributed Report

Create and modify distributed reports on a central manager.

## Before you begin

If you want to collect data from a group of managed units, verify that the group is defined.

## About this task

In this example, you'll see how to get a broader view and correlation insight for Exceptions (for example, SQL Errors) that are recorded on specific collectors.

This screen capture shows an example of a distributed report: Correlate Total Exceptions By User (Distributed). This view sums the total exceptions per user from all databases that are associated with the Guardium Managed Units selected for this Distributed Report. Likewise, you can view the Total Failed Login Attempts system wide, or the Total Exceptions per Source Programs.

| Date                    | User Name | Exception Type Description                | Sum Of Count of Exceptions |
|-------------------------|-----------|-------------------------------------------|----------------------------|
| 2014-03-19 08:00:00.8SA |           | Database Server returned an error 5890076 | 5890076                    |

In this specific example, the report data is gathered hourly - there is no need to wait at least an hour to get the initial results.

Note: The line saying 'Distributed Report status - click here for details', shows the status of data gathering, if data is missing from managed units then the line is colored in red; clicking the line navigates to details report of status per units per hour.

## Procedure

1. Click Reports > Report Configuration Tools > Distributed Report Builder.
  2. Click New.
  3. Select a report from the Based on Report drop-down list as the base for this distributed report. In this example, choose Exceptions Details.

## Distributed Report Configuration

Search

[Admin Dashboard TODO list stats - Distributed](#)

[Admin Dashboard VA stats - Distributed](#)

[Administrative Commands By User Dashboard-Distributed](#)

[Aggregation/Archive Log - Distributed](#)

[CCPA - Personal Data Objects Audit Trail-Distributed](#)

[CCPA z/OS - Personal Data Objects Audit Trail-Distributed](#)

[Enterprise Open Verification](#)

[New](#)
[Delete](#)
[Add to My Custom Reports](#)
[Log](#)

Based on Report

-----

## Gather Data From

● All Managed Units    ○ Group and Specific Managed Units

Group

All Aggregators  
All Collectors  
All Units group

Log

Based on Report \_\_\_\_\_

## Gather Data From

- In the Gather Data From section of the builder, choose All Managed Units (that the Central Manager is managing) or specify certain Group and Specific Managed Units, whose data will be included in the distributed report. If the Central Manager is also an Aggregator, it might need to be included. For this example, choose two groups from the Group list, and a few managed units from the Managed units list, but leave the 'Central Manager' unchecked.
  - In the Operation Mode, select the type of report: immediate or scheduled. The Immediate mode is mainly for online / real-time monitoring, such as, view the recent Failed Login Attempts, view recent Excessive Exception, or view real-time alerts. The Scheduled mode is an ongoing data-gathering that runs periodically based on the Schedule defined. This example summarizes the exceptions every hour. There is a requirement for filling in values for Exception Description and Destination Address.

## Operation Mode

Immediate  Schedule

Send Data To (primary)

Send Data To (secondary)

Time Granularity  Day

Purge After  Days

For Distributed Report in schedule mode, after clicking the Apply button, next define the schedule, and if needed, limit Roles.

Extraction is currently not scheduled.

### Roles

The Send data to and Send data to (secondary) fields define where distributed data is consolidated and made available for reports. By default, data is collected from managed units and made available on the central manager, but it is possible to send the data to any Guardium system using these fields. Send data to (secondary) defines a backup or secondary system where data is also sent. Either Send data to or Send data to (secondary) can identify a central manager, and it is possible for both fields to identify managed units if the data is not needed on a central manager.

6. Click Apply to create the Distributed Report.
7. Define the schedule by clicking Modify Schedule (this is mandatory to activate the process). A standard Schedule Definition window opens. Fill in all required details. See [Scheduling](#) for more information on scheduling.
8. Once applied, the new Distributed Report is added and highlighted in the list box.

## Distributed Report Configuration

Search

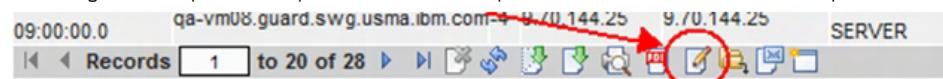
Aggregation/Archive Log - Distributed  
Enterprise Stap Verification  
**Exceptions Details-Distributed**  
Failed User Login Attempts - Distributed  
Scheduled Jobs - distributed  
Scheduled Jobs Exceptions - distributed

Based on Report : Exceptions Details

9. If you want to limit the roles for this report, click Roles to open the Assign Security Roles window; select the roles and click Apply.

## Results

The data is gathered from all the specified Managed Units and is stored in new designated entity (table). This entity is now available via the Query-Report Builder for use when creating additional queries. The option to build additional queries are available via the Distributed Report result screen as well. Click Edit the query for this report.



This default Report cannot be changed, click Clone, name it, remove all attributes and leave the Date, User Name, Exception Type Description, and Sum Of Count Of Exceptions.

## Working with API calls and reports

- [Mapping APIs to report results](#)

Guardium® comes with a battery of predefined reports and many of them are already mapped to GuardAPI functions to ease configuration. You can define additional reports, including custom reports, and map them to GuardAPI functions for each report.

- [How to Generate API Call from Reports](#)  
Generate Guard API calls from a report either from a single row within a report or based on the whole report
- [How to use Constants within API Calls](#)  
Create a new entity attribute to be used during an API function call.
- [How to use API Calls from Custom Reports](#)  
Link API functions to reports and map report fields to the API functional parameters.

## Mapping APIs to report results

Guardium® comes with a battery of predefined reports and many of them are already mapped to GuardAPI functions to ease configuration. You can define additional reports, including custom reports, and map them to GuardAPI functions for each report.

1. Open any predefined report from the Reports section.
2. From the Actions dropdown, select Add API mapping.
3. From Add API mapping, the following information displays:
  - Any API functions that are already mapped to this report. From Existing mapped API function, click Invoke to open a window from which you can enter the parameters for the selected function. You can either invoke the function immediately or generate and download a script to use as needed.
  - A search and filter mechanism to find the appropriate API command.
  - All of the API functions that are available to add to this report.
4. To add an API function, choose the function from the list, and then click Map Report Attributes to display the API-Report Parameter Mapping.
5. From API-Report Parameter Mapping, map the parameter name to the Report field.

Note: Sometimes you might want to include data that is not available in a Guardium report. In this case, you can create a constant to add to the report and use within the API parameter mappings. However, if you export a Guardium report that includes a constant, the constant is not exported.

To simplify the mapping between the GuardAPI parameters and Guardium attributes, the predefined report Query Entities & Attributes lists all of the Guardium attributes. This report provides a GUI interface and allows you to easily drill down from that report and create the linkages.

Existing Guardium attributes or user-defined constants can be mapped to the GuardAPI parameters of Existing Attributes or Constants.

Note: If a report has more than one GuardAPI attribute that is mapped to the same parameter, the API call picks the value in the first attribute (determined by the display order in the report).

### Mapping Existing Attributes

1. Go to the Query Entities & Attributes report to add the API parameter mappings. (Guardium Monitor > Query Entities & Attributes)
2. The Query Entities & Attributes report lists all of the Guardium attributes. Narrow down the records you are interested in by using Customize.
3. To create the mapping, double-click the attribute row to which to assign a parameter name.
4. Click Invoke.
5. Select the create\_api\_parameter\_mapping API function.
6. Enter the functionName and parameterName in the API Call Form.
7. Click Invoke now to create the API to Report Parameter Mapping.

For more information, see [How to use API calls from custom reports](#), which includes an example that maps GuardAPI parameters through the GUI.

### Mapping Constants

Sometimes you might want to include data that is not supplied within a Guardium report. For these instances, create a constant add it to the report, and then use it within the API parameter mappings.

1. Go to the Query Entities & Attributes report to add the API parameter mappings. (Guardium Monitor > Query Entities & Attributes).
2. The Query Entities & Attributes report is long because it lists all of the Guardium attributes. Narrow down the records you are interested in by using Customize.
3. To create a constant attribute, double-click any row for the entity for which you want to create a constant attribute.
4. Click Invoke.
5. Select the create\_constant\_attribute API.
6. Enter the constant value to use and specify the name (attributeLabel)
7. Click Invoke now to create the constant.
8. To create the mapping, double-click the newly created attribute row.
9. Click Invoke.
10. Select the create\_api\_parameter\_mapping API function.
11. Enter the functionName and parameterName in the API Call Form.
12. Click Invoke now to create the API to Report Parameter Mapping.
13. You must add the newly created attribute to the report. Modify the Query through the Query-Report Builder and add the field.

For more information, see [How to use Constants within API Calls](#), which includes an example to create and map a constant attribute through the GUI.

Note: If the Guardium report, with a constant added, is exported, the constant is not exported.

Note: When you use API mapping, table columns in a report appear in the report field whenever the table column is an attribute of an entity. Some of the columns, such as count column, are never displayed in the report field because it cannot be mapped.

## How to Generate API Call from Reports

Generate Guard API calls from a report either from a single row within a report or based on the whole report

Value-added: Through a GUI, by using existing data on the system that is displayed in reports as parameters for API calls, quickly and easily generate and populate API calls without having to perform system level commands or type lengthy API calls to quickly perform operations such as create datasources, define inspection engines, maintain user hierarchies, or maintain the Guardium features such as S-TAP.

Single Row API call

For this scenario, we will generate API function calls to populate the Data Security User Hierarchy.

1. To begin, let's show the current **Data Security User Hierarchy** for the user **scott**

The screenshot shows the 'Data Security User Hierarchy' window. On the left, there are dropdown menus for 'Roles' (set to 'All') and 'Users' (set to 'Knowitall, Scott (scott)'). Below these are two buttons: 'Refresh Cached Hierarchy' and 'Full Update Active User-DB Map'. On the right, a tree view displays a single node: 'User Knowitall, Scott (scott)'. A tooltip above the node says 'Parents : Click a node and right-click for options.' There is also a small icon of a person next to the node name.

2. To invoke an API function we must find a report that currently has the desired API functions linked to it. Since creating a user hierarchy is related to users, selection of a user report should yield good results. For this scenario we've selected the **User - Role** report.

The screenshot shows the 'User - Role' report interface. The title bar says 'User - Role'. The report table has columns: 'Login Name', 'Last Active', '# of Role', and '# of Users'. The data shows several users with their last active times, role counts, and user counts. At the bottom, there are navigation buttons and a toolbar with icons for print, copy, etc. A status bar at the bottom indicates 'Start Date: 2001-04-09 13:21:17 End Date: 2009-08-09 13:21:17' and 'REMOTE\_SOURCE'. The 'Aliases: OFF' option is checked.

3. Double-clicking on a row for drill-down will display an option to **Invoke...**

The screenshot shows the same 'User - Role' report interface. A context menu is open over the row for 'koopmann'. The menu items are 'Record Details' (disabled), 'Invoke...', and 'Delete'. The 'Invoke...' option is highlighted with a red box. The status bar at the bottom shows 'Start Date: 2001-04-09 13:21:17 End Date: 2009-08-09 13:21:17' and 'REMOTE\_SOURCE'. The 'Aliases: OFF' option is checked.

4. Click on the **Invoke...** option to display a list of API functions that are mapped to this report

The screenshot shows the same 'User - Role' report interface. The 'Invoke...' menu is open, displaying three API functions: 'create\_user\_hierarchy', 'delete\_user\_hierarchy\_by\_user', and 'list\_user\_hierarchy\_by\_parent\_user'. The 'create\_user\_hierarchy' option is highlighted with a red box. The status bar at the bottom shows 'Start Date: 2001-04-09 13:21:17 End Date: 2009-08-09 13:21:17' and 'REMOTE\_SOURCE'. The 'Aliases: OFF' option is checked.

5. Click on the **API** you'd like to invoke; bringing up the API Call Form for the Report and Invoked API Function.

6. Fill in the Required Parameters and any non-Required Parameters for the selected API call. Many of the parameters are pre-filled from the report but may be changed to build a unique API call. For specific help in filling out required or non-required parameters please see the individual API function calls within the GuardAPI Reference guide.

The screenshot shows the 'API Call Form' for the 'User - Role' report. The 'Report' field is set to 'User - Role' and the 'Api Function' field is set to 'create\_user\_hierarchy'. The form contains three input fields: 'userName' (set to 'jkoopmann'), 'parentUserName' (set to 'scott'), and 'api\_target\_host' (empty). Below these fields is a note: '\* Required parameter'. Underneath the fields are two dropdown menus: 'Log level' (set to '0') and 'Parameter to encrypt' (set to '-----'). At the bottom are two buttons: 'Generate script' and 'Invoke now'.

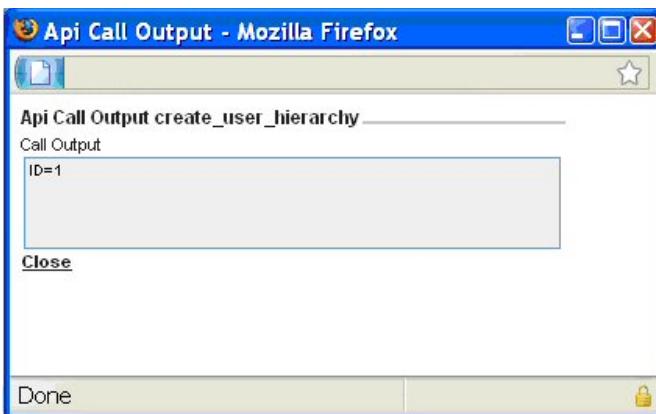
7. Use the drop-down list to select the **Log level**, where Log level represents the following (0 - returns ID=identifier and ERR=error\_code as defined in Return Codes, 1 - displays additional information to screen, 2 - puts information into the Guardium application debug logs, 3 - both 1 and 2).

8. Use the drop-down list to select a **Parameter to encrypt**.

Note: Parameter Encryption is enabled by setting the Shared Secret and is relevant only for invoking the API function through script generation.

9. Choose to **Invoke Now** or **Generate Script**.

- a. If **Invoke Now** is selected the API call will run immediately and display an API Call Output screen showing the status of the API call.



b. If **Generate Script** is selected: Open the generated script with your favorite editor or optionally save to disk to edit and execute at a later time -- replacing any of the empty parameter values (denoted by '< >') if contained within the script.

Note: Empty parameters may remain in the script as the API call will ignore them

Example Script

```
A template script for invoking guardAPI function create_user_hierarchy :

Usage: ssh cli@a1.corp.com<create_user_hierarchy_api_call.txt

replace any < > with the required value

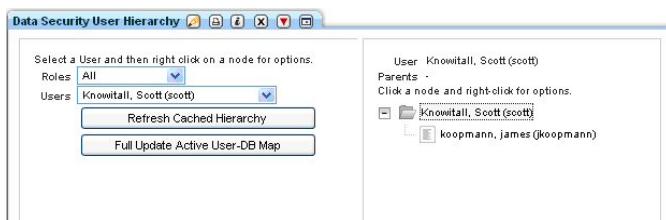
#
grdap create_user_hierarchy userName=jkoopmann parentUserName=scott
```

c. Execute the CLI function call.

Example Call

```
$ ssh cli@a1.corp.com<create_user_hierarchy_api_call.txt
```

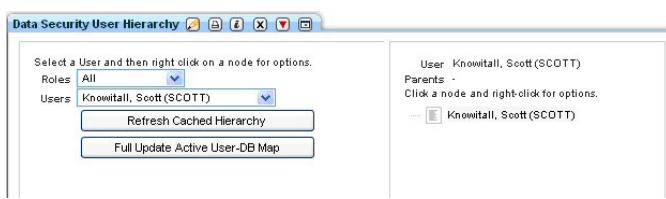
10. Validate. For this scenario it is a redisplay of the Data Security User Hierarchy.



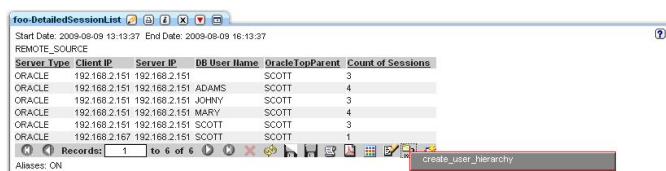
#### Multi Row API call

This scenario uses a custom report with mapped parameters to report fields. Please see additional scenarios further in this section for additional information.

1. To begin, let's show the current **Data Security User Hierarchy** for the user **scott**



2. Click on the **Invoke...** icon to display a list of APIs that are mapped to this report



3. Click on the **API** you'd like to invoke; bringing up the API Call Form for the Report and Invoked API Function. Invoking an API call from a report for multiple rows will produce an API Call Form that displays and enables the editing of all records displayed on the screen (dependent on the fetch size) to a maximum of 20 records.

Api Call Form - Mozilla Firefox

Report: foo-DetailedSessionList  
Api Function: create\_user\_hierarchy

| username *                                | parentUserName * |
|-------------------------------------------|------------------|
| <input checked="" type="checkbox"/> ADAMS | SCOTT            |
| <input checked="" type="checkbox"/> JOHNY | SCOTT            |
| <input checked="" type="checkbox"/> MARY  | SCOTT            |
| <input checked="" type="checkbox"/> SCOTT | SCOTT            |
| <input checked="" type="checkbox"/> SCOTT | SCOTT            |

\* Required parameter

Log level: 0 Parameter to encrypt: -----

Generate script    Invoke now

Done

4. Use the **check boxes** to select / de-select the rows that will be targeted for the API call.
5. Fill in the **Required Parameters** and any **non-Required Parameters** for the selected API call. Many of the parameters are pre-filled from the report but may be changed to build a unique API call. For specific help in filling out required or non-required parameters please see the individual API function calls within the GuardAPI Reference guide. Additionally, use the set of parameters for the API to enter a value for a parameter and then click the down arrow to populate that parameter for all records.
6. Use the drop-down list to select the **Log level**, where Log level represents the following (0 - returns ID=identifier and ERR=error\_code as defined in Return Codes, 1 - displays additional information to screen, 2 - puts information into the Guardium application debug logs, 3 - both 1 and 2).
7. Use the drop-down list to select a **Parameter to encrypt**.  
Note: Parameter Encryption is enabled by setting the Shared Secret and is relevant only for invoking the API function through script generation.

8. Choose to **Invoke Now** or **Generate Script**.

a. If **Invoke Now** is selected the API call runs immediately and displays an API Call Output screen showing the status of the API call. In this specific scenario the last two API calls would fail since we can not have a cyclical relationship in the hierarchy.

b. If **Generate Script** is selected: Open the generated script with your favorite editor or optionally save to disk to edit and execute at a later time. You can replace any of the empty parameter values (denoted by '< >') if contained within the script. With this scenario, we could easily delete the last two lines of the script -- knowing they would create cyclical errors.

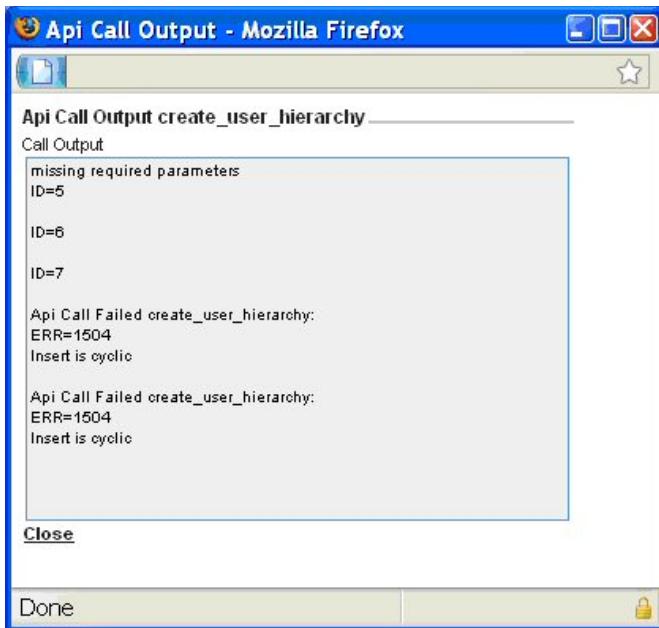
Note: Empty parameters are valid in the script since the API call ignores them.

Example Script

```
A template script for invoking guardAPI function create_user_hierarchy :
Usage: ssh cli@al.corp.com<create_user_hierarchy_api_call.txt
replace any < > with the required value
#
grdapi create_user_hierarchy userName=ADAMS parentUserName=SCOTT
grdapi create_user_hierarchy userName=JOHNY parentUserName=SCOTT
grdapi create_user_hierarchy userName=MARY parentUserName=SCOTT
grdapi create_user_hierarchy userName=SCOTT parentUserName=SCOTT
grdapi create_user_hierarchy userName=SCOTT parentUserName=SCOTT
```

Then Execute the CLI function call, for example:

```
$ ssh cli@al.corp.com<create_user_hierarchy_api_call.txt
```



9. Validate. For this scenario it is a re-display of the Data Security User Hierarchy.

## How to use Constants within API Calls

Create a new entity attribute to be used during an API function call.

Value-added: Through a GUI, create a user-defined constant that can be used for filling in a parameter in an API function call .

- From our report, we can modify it to have a field that we could use for parameter mappings.

| Server Type | Client IP     | Server IP     | DB User Name | Count of Sessions |
|-------------|---------------|---------------|--------------|-------------------|
| ORACLE      | 192.168.2.151 | 192.168.2.151 |              | 3                 |
| ORACLE      | 192.168.2.151 | 192.168.2.151 | ADAMS        | 4                 |
| ORACLE      | 192.168.2.151 | 192.168.2.151 | JOHNY        | 3                 |
| ORACLE      | 192.168.2.151 | 192.168.2.151 | MARY         | 4                 |
| ORACLE      | 192.168.2.151 | 192.168.2.151 | SCOTT        | 3                 |
| ORACLE      | 192.168.2.167 | 192.168.2.151 | SCOTT        | 1                 |

- Go to the Query Entities & Attributes report for the Client/Server entity within the ACCESS RULES VIOLATIONS domain. Double-click on a row and select the Invoke... option.

**Query Entities & Attributes**

DOMAIN\_LIKE LIKE % ENTITY\_LIKE LIKE Client/Server  
ATTRIBUTE\_LIKE LIKE %

| Domain Name             | Entity Label  | Attribute Label     |
|-------------------------|---------------|---------------------|
| ACCESS RULES VIOLATIONS | Client/Server | Alias Definition    |
| ACCESS RULES VIOLATIONS | Client/Server | Analyzed Client IP  |
| ACCESS RULES VIOLATIONS | Client/Server | Client Host Name    |
| ACCESS RULES VIOLATIONS | Client/Server | Client IP           |
| ACCESS RULES VIOLATIONS | Client/Server | Client MAC          |
| ACCESS RULES VIOLATIONS | Client/Server | Client OS           |
| ACCESS RULES VIOLATIONS | Client/Server | ClientIP-DBUser     |
| ACCESS RULES VIOLATIONS | Client/Server | DB Protocol         |
| ACCESS RULES VIOLATIONS | Client/Server | DB Protocol Version |
| ACCESS RULES VIOLATIONS | Client/Server | DB User Name        |
| ACCESS RULES VIOLATIONS | Client/Server | Network Protocol    |
| ACCESS RULES VIOLATIONS | Client/Server | OS User             |
| ACCESS RULES VIOLATIONS | Client/Server | Server Description  |
| ACCESS RULES VIOLATIONS | Client/Server | Server Host Name    |
| ACCESS RULES VIOLATIONS | Client/Server | Server IP           |
| ACCESS RULES VIOLATIONS | Client/Server | Server OS           |
| ACCESS RULES VIOLATIONS | Client/Server | Server Type         |
| ACCESS RULES VIOLATIONS | Client/Server | ServerIP-DBUser     |
| ACCESS RULES VIOLATIONS | Client/Server | Service Name        |
| ACCESS RULES VIOLATIONS | Client/Server | Source Program      |

Records: 1 to 20 of 150 Aliases: ON

3. Invoke the API function create\_constant\_attribute.

**Query Entities & Attributes**

DOMAIN\_LIKE LIKE % ENTITY\_LIKE Client/Server  
ATTRIBUTE\_LIKE LIKE %

| Domain Name             | Entity Label  | Attribute Label     |
|-------------------------|---------------|---------------------|
| ACCESS RULES VIOLATIONS | Client/Server | Access Id           |
| ACCESS RULES VIOLATIONS | Client/Server | Analyzed Client IP  |
| ACCESS RULES VIOLATIONS | Client/Server | Client Host Name    |
| ACCESS RULES VIOLATIONS | Client/Server | Client IP           |
| ACCESS RULES VIOLATIONS | Client/Server | Client MAC          |
| ACCESS RULES VIOLATIONS | Client/Server | Client OS           |
| ACCESS RULES VIOLATIONS | Client/Server | ClientIP-DBUser     |
| ACCESS RULES VIOLATIONS | Client/Server | DB Protocol         |
| ACCESS RULES VIOLATIONS | Client/Server | DB Protocol Version |
| ACCESS RULES VIOLATIONS | Client/Server | DB User Name        |
| ACCESS RULES VIOLATIONS | Client/Server | Network Protocol    |
| ACCESS RULES VIOLATIONS | Client/Server | OS User             |
| ACCESS RULES VIOLATIONS | Client/Server | Server Description  |
| ACCESS RULES VIOLATIONS | Client/Server | Server Host Name    |
| ACCESS RULES VIOLATIONS | Client/Server | Server IP           |
| ACCESS RULES VIOLATIONS | Client/Server | Server OS           |
| ACCESS RULES VIOLATIONS | Client/Server | Server Type         |
| ACCESS RULES VIOLATIONS | Client/Server | ServerIP-DBUser     |
| ACCESS RULES VIOLATIONS | Client/Server | Service Name        |
| ACCESS RULES VIOLATIONS | Client/Server | Source Program      |

Records: 1 to 20 of 150 Aliases: ON

4. Fill in the constant value to use ('SCOTT'), fill in the attributeLabel you like to name it ('OracleTopParent'), and then click on the Invoke now button to create the constant.

**Api Call Form - Mozilla Firefox**

Report: Query Entities & Attributes  
Api Function: create\_constant\_attribute

|                |                 |
|----------------|-----------------|
| constant       | SCOTT           |
| entityLabel    | Client/Server   |
| attributeLabel | OracleTopParent |

\* Required parameter

Log level: 0 Parameter to encrypt: -----

Generate script    **Invoke now**

Done

5. Clicking on the Invoke now button will produce a API Call Output status showing the constant was created.

**Api Call Output create\_constant\_attribute**

Call Output

```
ID=20000
Constant SCOTT Created
```

6. A re-display of the Query Entities & Attributes report will show the new attribute created.

| Domain Name             | Entity Label  | Attribute Label     |
|-------------------------|---------------|---------------------|
| ACCESS RULES VIOLATIONS | Client/Server | Access Id           |
| ACCESS RULES VIOLATIONS | Client/Server | Analyzed Client IP  |
| ACCESS RULES VIOLATIONS | Client/Server | Client Host Name    |
| ACCESS RULES VIOLATIONS | Client/Server | Client IP           |
| ACCESS RULES VIOLATIONS | Client/Server | Client MAC          |
| ACCESS RULES VIOLATIONS | Client/Server | Client OS           |
| ACCESS RULES VIOLATIONS | Client/Server | ClientIP-DBUser     |
| ACCESS RULES VIOLATIONS | Client/Server | DB Protocol         |
| ACCESS RULES VIOLATIONS | Client/Server | DB Protocol Version |
| ACCESS RULES VIOLATIONS | Client/Server | DB User Name        |
| ACCESS RULES VIOLATIONS | Client/Server | Network Protocol    |
| ACCESS RULES VIOLATIONS | Client/Server | OracleTopParent     |
| ACCESS RULES VIOLATIONS | Client/Server | OS User             |
| ACCESS RULES VIOLATIONS | Client/Server | Server Description  |
| ACCESS RULES VIOLATIONS | Client/Server | Server Host Name    |
| ACCESS RULES VIOLATIONS | Client/Server | Server IP           |
| ACCESS RULES VIOLATIONS | Client/Server | Server OS           |
| ACCESS RULES VIOLATIONS | Client/Server | Server Type         |
| ACCESS RULES VIOLATIONS | Client/Server | ServerIP-DBUser     |
| ACCESS RULES VIOLATIONS | Client/Server | Service Name        |

7. The newly created constant can now be mapped for the report. Double-click on the new row and select the Invoke... option.

| Domain Name             | Entity Label  | Attribute Label     |
|-------------------------|---------------|---------------------|
| ACCESS RULES VIOLATIONS | Client/Server | Access Id           |
| ACCESS RULES VIOLATIONS | Client/Server | Analyzed Client IP  |
| ACCESS RULES VIOLATIONS | Client/Server | Client Host Name    |
| ACCESS RULES VIOLATIONS | Client/Server | Client IP           |
| ACCESS RULES VIOLATIONS | Client/Server | Client MAC          |
| ACCESS RULES VIOLATIONS | Client/Server | Client OS           |
| ACCESS RULES VIOLATIONS | Client/Server | ClientIP-DBUser     |
| ACCESS RULES VIOLATIONS | Client/Server | DB Protocol         |
| ACCESS RULES VIOLATIONS | Client/Server | DB Protocol Version |
| ACCESS RULES VIOLATIONS | Client/Server | DB User Name        |
| ACCESS RULES VIOLATIONS | Client/Server | Network Protocol    |
| ACCESS RULES VIOLATIONS | Client/Server | OracleTopParent     |
| ACCESS RULES VIOLATIONS | Client/Server | OS User             |
| ACCESS RULES VIOLATIONS | Client/Server | Alias Definition    |
| ACCESS RULES VIOLATIONS | Client/Server | Invoke...           |
| ACCESS RULES VIOLATIONS | Client/Server | Server Descri       |
| ACCESS RULES VIOLATIONS | Client/Server | Server Host Name    |
| ACCESS RULES VIOLATIONS | Client/Server | Server IP           |
| ACCESS RULES VIOLATIONS | Client/Server | Server OS           |
| ACCESS RULES VIOLATIONS | Client/Server | Server Type         |
| ACCESS RULES VIOLATIONS | Client/Server | ServerIP-DBUser     |
| ACCESS RULES VIOLATIONS | Client/Server | Service Name        |

8. Select the create\_api\_parameter\_mapping option.

| Domain Name             | Entity Label  | Attribute Label                 |
|-------------------------|---------------|---------------------------------|
| ACCESS RULES VIOLATIONS | Client/Server | Access Id                       |
| ACCESS RULES VIOLATIONS | Client/Server | Analyzed Client IP              |
| ACCESS RULES VIOLATIONS | Client/Server | Client Host Name                |
| ACCESS RULES VIOLATIONS | Client/Server | Client IP                       |
| ACCESS RULES VIOLATIONS | Client/Server | Client MAC                      |
| ACCESS RULES VIOLATIONS | Client/Server | Client OS                       |
| ACCESS RULES VIOLATIONS | Client/Server | ClientIP-DBUser                 |
| ACCESS RULES VIOLATIONS | Client/Server | DB Protocol                     |
| ACCESS RULES VIOLATIONS | Client/Server | DB Protocol Version             |
| ACCESS RULES VIOLATIONS | Client/Server | DB User Name                    |
| ACCESS RULES VIOLATIONS | Client/Server | Network Protocol                |
| ACCESS RULES VIOLATIONS | Client/Server | OS User                         |
| ACCESS RULES VIOLATIONS | Client/Server | create_constant_attribute       |
| ACCESS RULES VIOLATIONS | Client/Server | create_api_parameter_mapping    |
| ACCESS RULES VIOLATIONS | Client/Server | delete_api_parameter_mapping    |
| ACCESS RULES VIOLATIONS | Client/Server | list_param_mapping_for_function |
| ACCESS RULES VIOLATIONS | Client/Server | Server Descri                   |
| ACCESS RULES VIOLATIONS | Client/Server | Server Host Name                |
| ACCESS RULES VIOLATIONS | Client/Server | Server IP                       |
| ACCESS RULES VIOLATIONS | Client/Server | Server OS                       |
| ACCESS RULES VIOLATIONS | Client/Server | Server Type                     |
| ACCESS RULES VIOLATIONS | Client/Server | ServerIP-DBUser                 |
| ACCESS RULES VIOLATIONS | Client/Server | Service Name                    |
| ACCESS RULES VIOLATIONS | Client/Server | Source Program                  |

9. Fill in the functionName and the parameterName and click on the Invoke now button.

Api Call Form - Mozilla Firefox:

Report: Query Entities & Attributes  
Api Function: create\_api\_parameter\_mapping

|                 |                        |
|-----------------|------------------------|
| functionName    | create_user_hierarchy  |
| parameterName   | parentUserName         |
| domain          | ACCESS RULES VIOLATION |
| entityLabel     | Client/Server          |
| attributeLabel  | OracleTopParent        |
| api_target_host |                        |

\*Required parameter

Log level: 0

Parameter Encryption not enabled - shared secret not set.

Generate script    Invoke now

Done

10. The newly created attribute must be added to the report. Edit the query through Query Builder and add the field.

The screenshot displays two instances of the Query Builder application window. Both windows show a hierarchical navigation pane on the left with categories like 'Session', 'Application Events', 'SQL', and 'Command'. The main area contains a 'foo-DetailedSessionList' report. In the first window (left), a context menu is open over the 'OracleTopParent' attribute in the 'Query Conditions' pane, with options like 'Add Field', 'Add Condition', 'Remove', 'Clone', 'Roles...', 'Save', and 'Back'. The second window (right) shows the same setup but without the context menu open.

11. Now when the report is displayed the new attribute is displayed.

| foo-DetailedSessionList                                                        |               |               |              |                 |                   |
|--------------------------------------------------------------------------------|---------------|---------------|--------------|-----------------|-------------------|
| Start Date: 2009-08-09 13:07:42 End Date: 2009-08-09 16:07:42<br>REMOTE_SOURCE |               |               |              |                 |                   |
| Server Type                                                                    | Client IP     | Server IP     | DB User Name | OracleTopParent | Count of Sessions |
| ORACLE                                                                         | 192.168.2.151 | 192.168.2.151 | SCOTT        | 3               |                   |
| ORACLE                                                                         | 192.168.2.151 | 192.168.2.151 | ADAMS        | SCOTT           | 4                 |
| ORACLE                                                                         | 192.168.2.151 | 192.168.2.151 | JOHNNY       | SCOTT           | 3                 |
| ORACLE                                                                         | 192.168.2.151 | 192.168.2.151 | MARY         | SCOTT           | 4                 |
| ORACLE                                                                         | 192.168.2.151 | 192.168.2.151 | SCOTT        | SCOTT           | 3                 |
| ORACLE                                                                         | 192.168.2.167 | 192.168.2.151 | SCOTT        | SCOTT           | 1                 |

12. To validate the new constant's usage, double-click on a row and select the Invoke... option.

| foo-DetailedSessionList                                                        |               |               |              |                 |                   |
|--------------------------------------------------------------------------------|---------------|---------------|--------------|-----------------|-------------------|
| Start Date: 2009-08-09 13:07:42 End Date: 2009-08-09 16:07:42<br>REMOTE_SOURCE |               |               |              |                 |                   |
| Server Type                                                                    | Client IP     | Server IP     | DB User Name | OracleTopParent | Count of Sessions |
| ORACLE                                                                         | 192.168.2.151 | 192.168.2.151 | SCOTT        | 3               |                   |
| ORACLE                                                                         | 192.168.2.151 | 192.168.2.151 | ADAMS        | SCOTT           | 4                 |
| ORACLE                                                                         | 192.168.2.151 | 192.168.2.151 | JOHNNY       | SCOTT           | 3                 |
| ORACLE                                                                         | 192.168.2.151 | 192.168.2.151 | MARY         | SCOTT           | 4                 |
| ORACLE                                                                         | 192.168.2.151 | 192.168.2.151 | SCOTT        | SCOTT           | 3                 |
| ORACLE                                                                         | 192.168.2.167 | 192.168.2.151 | SCOTT        | SCOTT           | 1                 |

A context menu is open over the 'JOHNNY' row in the table, listing various reporting options:

- Admin Users Sessions
- Client IP Activity Summary
- DB Predefined Users Sessions
- DB Server Throughput-Chart
- Detailed Sessions List
- Exceptions Type Distribution
- Full SQL By Client IP
- Full SQL By DB User
- Sessions By Client IP
- Sessions By Server IP
- Sessions By Source Program
- Sessions By User
- Sessions Details By Server
- Throughput-Chart
- User Activity Summary
- Alias Definition
- Invoke...

13. Select the API function

| Server Type | Client IP     | Server IP     | DB User Name | OracleTopParent | Count of Sessions |
|-------------|---------------|---------------|--------------|-----------------|-------------------|
| ORACLE      | 192.168.2.151 | 192.168.2.151 | ADAMS        | SCOTT           | 3                 |
| ORACLE      | 192.168.2.151 | 192.168.2.151 | JOHNY        | SCOTT           | 3                 |
| ORACLE      | 192.168.2.151 | 192.168.2.151 | MARY         | SCOTT           | 4                 |
| ORACLE      | 192.168.2.151 | 192.168.2.151 | SCOTT        | SCOTT           | 3                 |
| ORACLE      | 192.168.2.151 | 192.168.2.151 | SCOTT        | SCOTT           | 1                 |

14. Now the parentUserName is populated from the newly added constant. Click the Invoke now button.

Report: foo-DetailedSessionList  
Api Function: create\_user\_hierarchy

userName: JOHNY \*  
parentUserName: SCOTT \*

\* Required parameter

Log level: 0 Parameter to encrypt: -----

Generate script    Invoke now

Done

15. Validate the new Data Security User Hierarchy.

Select a User and then right click on a node for options.

Roles: All  
Users: Knowitall, Scott (SCOTT)

Parents: Click a node and right-click for options.

- User: Knowitall, Scott (SCOTT)
  - Parents:
  - Click a node and right-click for options.
  - Nodes:
    - Knowitall, Scott (SCOTT)
    - Cat, Johny (JOHNY)
    - koopmann, james (koopmann)
    - Smith, Adams (ADAMS)

## How to use API Calls from Custom Reports

Link API functions to reports and map report fields to the API functional parameters.

Value-added: Through a GUI, quickly and easily map API parameters to custom report fields to be used in API function calls.

By default, a newly created custom report does not have any API functions linked to it. Linking API functions to reports is done through Guardium's Query-Report Builder

1. Open the Query-Report Builder, find your custom report, and then click on the API Assignment button.
2. The API Assignment panel shows all the API functions assigned to the selected report. Notice for our scenario the report selected has no API functions assigned to it.

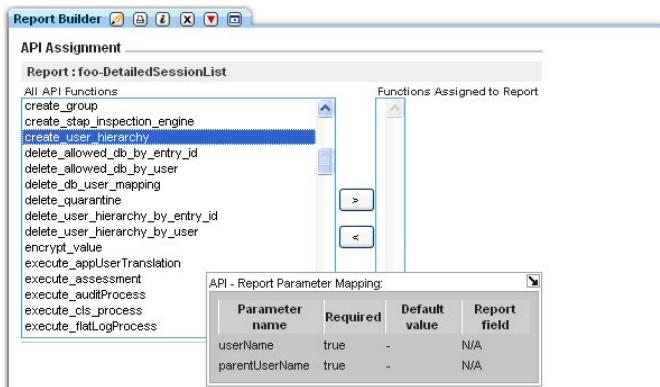
Report : foo-DetailedSessionList

All API Functions

Functions Assigned to Report

Back    Apply

3. To assign an API function to a report, find an API you'd like to link to the report, click the greater than arrow, and then click the apply button. For our scenario we selected create\_user\_hierarchy. When selected a pop-up window will appear that shows the report parameter mappings (which report fields will be used when calling the API function). Notice there are no mapped report fields to parameter names.



4. At this point, none of the report fields are mapped to the API parameters. Users can go to the Query Entities & Attributes report to create these mappings, otherwise when invoking the API call none of the parameters will have values. add the API parameter mappings. Open the Query Entities & Attributes report and create the mappings. Since our report for this scenario uses the Client/Server entity within the ACCESS RULES VIOLATIONS domain, filter the report by using the customize button; modifying the report to display only the Client/Server entity.

| Query Entities & Attributes                                           |               |                     |
|-----------------------------------------------------------------------|---------------|---------------------|
| DOMAIN_LIKE LIKE % ENTITY_LIKE Client/Server<br>ATTRIBUTE_LIKE LIKE % |               |                     |
| Domain Name                                                           | Entity Label  | Attribute Label     |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Access Id           |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Analyzed Client IP  |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Client Host Name    |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Client IP           |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Client MAC          |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Client OS           |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Client IP-DBUser    |
| ACCESS RULES VIOLATIONS                                               | Client/Server | DB Protocol         |
| ACCESS RULES VIOLATIONS                                               | Client/Server | DB Protocol Version |
| ACCESS RULES VIOLATIONS                                               | Client/Server | DB User Name        |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Network Protocol    |
| ACCESS RULES VIOLATIONS                                               | Client/Server | OS User             |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Server Description  |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Server Host Name    |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Server IP           |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Server OS           |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Server Type         |
| ACCESS RULES VIOLATIONS                                               | Client/Server | ServerIP-DBUser     |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Service Name        |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Source Program      |

5. Double-click on the attribute you'd like to assign to a parameter name and click on the Invoke... option.

| Query Entities & Attributes                                           |               |                     |
|-----------------------------------------------------------------------|---------------|---------------------|
| DOMAIN_LIKE LIKE % ENTITY_LIKE Client/Server<br>ATTRIBUTE_LIKE LIKE % |               |                     |
| Domain Name                                                           | Entity Label  | Attribute Label     |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Access Id           |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Analyzed Client IP  |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Client Host Name    |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Client IP           |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Client MAC          |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Client OS           |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Client IP-DBUser    |
| ACCESS RULES VIOLATIONS                                               | Client/Server | DB Protocol         |
| ACCESS RULES VIOLATIONS                                               | Client/Server | DB Protocol Version |
| ACCESS RULES VIOLATIONS                                               | Client/Server | DB User Name        |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Network Protocol    |
| ACCESS RULES VIOLATIONS                                               | Client/Server | OS User             |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Server Description  |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Server Host Name    |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Server IP           |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Server OS           |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Server Type         |
| ACCESS RULES VIOLATIONS                                               | Client/Server | ServerIP-DBUser     |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Service Name        |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Source Program      |

6. Select the create\_api\_parameter\_mapping API function.

| Query Entities & Attributes                                           |               |                     |
|-----------------------------------------------------------------------|---------------|---------------------|
| DOMAIN_LIKE LIKE % ENTITY_LIKE Client/Server<br>ATTRIBUTE_LIKE LIKE % |               |                     |
| Domain Name                                                           | Entity Label  | Attribute Label     |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Access Id           |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Analyzed Client IP  |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Client Host Name    |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Client IP           |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Client MAC          |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Client OS           |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Client IP-DBUser    |
| ACCESS RULES VIOLATIONS                                               | Client/Server | DB Protocol         |
| ACCESS RULES VIOLATIONS                                               | Client/Server | DB Protocol Version |
| ACCESS RULES VIOLATIONS                                               | Client/Server | DB User Name        |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Network Protocol    |
| ACCESS RULES VIOLATIONS                                               | Client/Server | OS User             |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Server Description  |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Server Host Name    |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Server IP           |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Server OS           |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Server Type         |
| ACCESS RULES VIOLATIONS                                               | Client/Server | ServerIP-DBUser     |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Service Name        |
| ACCESS RULES VIOLATIONS                                               | Client/Server | Source Program      |

7. Fill in the functionName and parameterName in the API Call Form and click on the Invoke now button.

Report: Query Entities & Attributes  
Api Function: create\_api\_parameter\_mapping

|                 |                        |
|-----------------|------------------------|
| functionName    | create_user_hierarchy  |
| parameterName   | userName               |
| domain          | ACCESS RULES VIOLATION |
| entityLabel     | Client/Server          |
| attributeLabel  | DB User Name           |
| api_target_host |                        |

\*Required parameter  
Log level: 0  
Parameter Encryption not enabled - shared secret not set.  
Generate script    Invoke now

8. Now, when we go back to the Report Builder for our report and look at the API Assignment; clicking on the create\_user\_hierarchy API function displays the API - Report Parameter Mapping with our mapping of userName to the Report field Client/Server.DB User Name.

Report Builder

Report : foo-DetailedSessionList

API Assignment

|                                |   |
|--------------------------------|---|
| create_constant_attribute      | > |
| create_datasource              | < |
| create_datasourceRef_by_id     |   |
| create_datasourceRef_by_name   |   |
| create_group                   |   |
| create_stap_inspection_engine  |   |
| create_user_hierarchy          |   |
| delete_allowed_db_by_entry_id  |   |
| delete_allowed_db_by_user      |   |
| delete_db_user_mapping         |   |
| delete_quarantine              |   |
| delete_user_hierarchy_by_entry |   |
| delete_user_hierarchy_by_user  |   |
| encrypt_value                  |   |
| execute_appUserTranslation     |   |

API - Report Parameter Mapping:

| Parameter name | Required | Default value | Report field               |
|----------------|----------|---------------|----------------------------|
| userName       | true     | -             | Client/Server.DB User Name |
| parentUserName | true     | -             | N/A                        |

9. Click on the greater-than arrow '>' and click the Apply button

Report Builder

Report : foo-DetailedSessionList

API Assignment

|                              |   |
|------------------------------|---|
| add_api_parameter_mapping    | > |
| add_cas_host_instance        |   |
| add_db_user_mapping          |   |
| add_entry_location           |   |
| add_member_to_group_by_desc  |   |
| add_member_to_group_by_id    |   |
| add_quarantine_allowed_until |   |
| add_quarantine_until         |   |
| copy_rules                   |   |
| create_allowed_db            |   |
| create_constant_attribute    |   |
| create_datasource            |   |
| create_datasourceRef_by_id   |   |
| create_datasourceRef_by_name |   |
| create_group                 |   |

10. Now when we invoke the create\_user\_hierarchy API function through our report the parameter userName will be populated from the report. To see this, go back to the report and double-click on a row and then click on the Invoke... option.

foo-DetailedSessionList

Start Date: 2009-08-09 12:36:31 End Date: 2009-08-09 15:36:31

REMOTE\_SOURCE

| Server Type | Client IP     | Server IP     | DB User Name | Count of Sessions |
|-------------|---------------|---------------|--------------|-------------------|
| ORACLE      | 192.168.2.151 | 192.168.2.151 | ADA          | 3                 |
| ORACLE      | 192.168.2.151 | 192.168.2.151 | JOHN         | 1                 |
| ORACLE      | 192.168.2.151 | 192.168.2.151 | MAR          | 1                 |
| ORACLE      | 192.168.2.151 | 192.168.2.151 | SCO          | 1                 |
| ORACLE      | 192.168.2.167 | 192.168.2.151 | SCO          | 1                 |

Records: 1 to 6 of 6

Aliases: ON

Invoke...

Detailed Sessions List  
Exceptions Type Distribution  
Full SQL By Client IP  
Full SQL By DB User  
Sessions By Client IP  
Sessions By Server IP  
Sessions By Source Program  
Sessions By User  
Sessions Details By Server  
Throughput-Chart  
User Activity Summary  
Alias Definition

11. Click on the API function (in our case create\_user\_hierarchy).

| Server Type | Client IP     | Server IP     | DB User Name | Count of Sessions |
|-------------|---------------|---------------|--------------|-------------------|
| ORACLE      | 192.168.2.151 | 192.168.2.151 | ADAMS        | 4                 |
| ORACLE      | 192.168.2.151 | 192.168.2.151 | JOHNV        | 3                 |
| ORACLE      | 192.168.2.151 | 192.168.2.151 | MARY         | 4                 |
| ORACLE      | 192.168.2.151 | 192.168.2.151 | SCOTT        | 3                 |
| ORACLE      | 192.168.2.167 | 192.168.2.151 | SCOTT        | 1                 |

create\_user\_hierarchy

12. Notice that the userName is now populated from the report field.

Report: foo-DetailedSessionList  
Api Function: create\_user\_hierarchy

userName ADAMS \*

parentUserName SCOTT \*

\* Required parameter

Log level: 0 Parameter to encrypt: -----

Generate script    Invoke now

Done

13. Fill in the parentUserName and click the Invoke now button.

Report: foo-DetailedSessionList  
Api Function: create\_user\_hierarchy

userName ADAMS \*

parentUserName SCOTT \*

\* Required parameter

Log level: 0 Parameter to encrypt: -----

Generate script    Invoke now

Done

14. Verify that the new Data Security User Hierarchy has been added.

Select a User and then right click on a node for options.  
Roles: All  
Users: Knowitall, Scott (SCOTT)

User Knowitall, Scott (SCOTT)  
Parents: -  
Click a node and right-click for options.  
[ ] Knowitall, Scott (SCOTT)  
[ ] koopmann, james (koopmann)  
[ ] Smith, Adams (ADAMS)

## Working with external feeds

Use external feeds to send Guardium report data directly to an external database. Sending reporting data to an external database is useful in several scenarios, for example when combining or correlating Guardium data with non-Guardium data, when using Guardium data with external tools, or when machine-parsing records in especially large reports.

- [Mapping an External Feed](#)  
Learn how to map an external feed to send Guardium report data directly to an external database.
- [Creating an external feed](#)  
An external feed task defines the task and the target external database.

## Mapping an External Feed

Learn how to map an external feed to send Guardium report data directly to an external database.

### Before you begin

Verify the following prerequisites before mapping an external feed:

- Identify the external database that will receive data from the feed, and gather the connection information required for that database (ip address, port number, username, password, etc.). External feeds currently support relational databases and may not function with other database types.
- Identify the Guardium report that will provide data to the external feed.

## About this task

External feeds allow you to send Guardium report information directly to an external database. Anything that can be defined in a report can be sent via an external feed. These feeds depend on mapping DOMAIN\_ID and ATTRIBUTE\_ID from Guardium's reporting mechanism to table fields on the external database. Each mapping consists of the records in four tables (EF\_MAP\_TYPE\_HDR, EF\_MAP\_TABLE, EF\_MAP\_COLUMN, and EF\_MAP\_GDM\_TYPE). Use the `grdapicreate_ef_mapping` function to help create these tables and establish the mapping.

## Procedure

1. Generate a report with the data you would like to transfer using an external feed. You can do this from a central manager, aggregator, or stand-alone Guardium instance, provided that system can access the report data you require.
2. From the CLI, run `grdapicreate_ef_mapping reportName="My report"`. In addition to establishing the mapping, the `grdapicreate_ef_mapping` function also generates a sample `create table` statement to be used in subsequent steps.
3. On the Guardium system where your report is defined, search `/var/log/guard` for a filename like `ef_sample_[my_report].sql`. This file contains the example `create table` statements. You must modify the statements in this file to match the requirements of your external database. After modifying the file, run the statements against your external database to create the target tables.

## Results

The external feed should now be available for use in workflow processes defined through the audit process builder. Continue with [Creating an external feed](#).

## Creating an external feed

An external feed task defines the task and the target external database.

Before using external feeds, verify the following prerequisites:

- [Mapping an External Feed](#): Map a feed between Guardium and an external database. External feeds currently support relational databases and may not function with other database types.
- The External Data Feed is an optional component. It must be enabled (by product key), or else you cannot create an external feed.
- Create a report defining the data to send via the external feed. Predefined reports do not work with external feeds. If you want to use a predefined reports, make a copy with the report and use the copy for the external feed.

The first time that an optional external feed task runs, the necessary internal representation of the audit sources are created. One limitation is that data that is timestamped with a date earlier than the audit source creation date cannot be stored. This means that the first time the task runs, it only exports data for the current date. On subsequent executions of the task, following that date, any data from that date forward can be exported. (In other words, the next day, you can export that day's data plus the prior day's data.)

If you have not yet started to define a compliance workflow automation process, see [Create a Workflow Process](#) before performing this procedure.

1. Navigate to Comply > Tools and Views > Audit Process Builder and click . The Create New Audit Process window opens.
2. Type in the name of the process.
3. Open the Add Tasks row and click .
4. From the Task Type drop-down list, select External Feed. The New Task window refreshes with the External Feed parameters.
5. Fill in the parameters:
  - Name: a unique task name
  - Feed Type: (The controls that appear next depend on the feed type selected.)
  - External Feed Event:
  - Report: the report Depending on the report selected, a variable number of parameters appear in the Task Parameters pane.
  - In the Extract Lag box, enter the number of hours by which the feed is to lag, and mark the Continuous box to include data up to the time that the audit task runs. Extract Log only works when the Continuous box is marked.
  - Datasource: identify one or more datasources for the external feed, or create a new datasource by clicking .
  - Enter all parameter values in the Task Parameters pane. The parameters vary depending on the report selected. Count column is not supported in External Feed.
6. Click OK.

## Related concepts

- [Building audit processes](#)

## Related tasks

- [Mapping an External Feed](#)

## Creating reports for z/OS

Learn how to create Guardium reports for z/OS data sources by customizing built-in reports and example queries.

While the process of creating reports for z/OS data sources is the same as for other databases, there is not always a direct mapping between mainframe concepts and Guardium's reporting entities and attributes. To ease communication between auditors and mainframe personnel, this section outlines the mapping of mainframe event data to Guardium entities and attributes. There are some built-in reports that can be customized, and this information describes additional queries that are useful for typical auditing scenarios.

## Related concepts

- [Domains, Entities, and Attributes](#)
- [Using the Query-Report Builder](#)
- [Entities and Attributes in the domains](#)

## Built-in reports for Data Sets

### DATA SET Access

This report is based on a main entity of "object". This means that the report has one line for each object (data set). So if you have an access command (Verb) with multiple objects, the command will appear in the report multiple times, once for each object.

The extra rows can be skipped if you check 'add distinct' in the Query-Report Builder for the report.

Note: This report does have customized column names to make the report more readable. By editing the report query and comparing with the report headers, you can see the differences.

Example: Instead of SQL Verb, the column is Action. And instead of DB Protocol, the column is Event Type.

If you like the built-in query and want to further customize the report, you can go to Report Builder to clone the report definition and customize the column headers.

### DATA SET Access

This report is based on the Full SQL main entity and includes a pretty complete set of attributes for data set and record level access.

Recommendation: Clone this query and make the following modifications:

- Move the timestamp to the first column.
- Add the full SQL ID column to enable very detailed sorting if timestamp granularity is not fine enough.
- Review the query conditions in the query. If you want to use the same report for other databases, such as IMS, you may want to make the DB Protocol field a Parameter instead of a value.

## Report entities and attributes for Data Sets

Use this information to find reporting attributes for Data Sets.

Table 1. Attributes for Client/Server Entity (Data Sets)

| Attribute          | Description                                                                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Timestamp          | All attributes in this session are static, so this timestamp is created only once, when Guardium observes a request on the defined connection for the first time. |
| Service Name       | LPAR.                                                                                                                                                             |
| Server Description | Not populated.                                                                                                                                                    |
| DB User Name       | Not populated. Use the following attributes from the Full SQL entity instead: IMS/DATA SET User ID or VSAM RLM CICS User ID (for RLM only)                        |
| Server Type        | DATA SET. IMS. If more than one type of database is writing events to the Guardium system, this field helps separate the events.                                  |
| Server IP          | IP Address of LPAR.                                                                                                                                               |
| Server Host Name   | Hostname of LPAR.                                                                                                                                                 |
| Client IP          | IP address of S-TAP. Usually the same as the Server IP.                                                                                                           |
| Network Protocol   | Type of access. <ul style="list-style-type: none"><li>• DATA SET</li><li>• DATA SET Record Level Monitoring (RLM)</li></ul>                                       |
| DB Protocol        | DATA SET                                                                                                                                                          |
| Source Program     | Job type:<br>STC – Started Task<br>TSU-Time sharing user<br>JOB-Batch job<br>APPC – Advanced Program-to-Program communication)<br>OMVS- Unix System Services      |

Table 2. Attributes for Session Entity (Data Sets)

| Attribute  | Description                                                                                                                                                                           |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Timestamp  | Initially, a timestamp created for the first request on a connection. Later, it is updated when it is marked inactive following an extended period of time with no observed activity. |
| Session ID | Unique identifier generated by Guardium. Because IMS does not have the concept of 'sessions', this is not particularly meaningful in IMS reporting.                                   |

| Attribute | Description                                                        |
|-----------|--------------------------------------------------------------------|
| Access ID | Uniquely identifies the access period for this line of the report. |

Table 3. Attributes for Access Period Entity (Data Sets). This entity provides no useful information for Data Sets monitoring.

| Attribute              | Description                                                                                                                                                                                                                 |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application User       | Not used for Data Sets                                                                                                                                                                                                      |
| Failed SQLs            | Not used for Data Sets                                                                                                                                                                                                      |
| Total Records Affected | Not used. You will see -1 in this field. If you are interested in seeing how many records are affected for VSAM data sets, see the Data Set Records Inserted, Updated, Deleted and Retrieved fields in the Full SQL entity. |
| Successful SQLs        | Not used.                                                                                                                                                                                                                   |

Table 4. Attributes for Full SQL Entity (Data Sets)

| Attribute                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Full SQL                             | Contains almost all information about an event. Computed attributes for other report fields are created from this data, which includes:<br>uid=; prog=; job=; step=; step#=; job#=; ugid=; rec_dlt=; rec_del=; rec_ins=; rec_upd=; rec_ret=; pre=; desc=; type=; dbd=; dsn=; smf_accs=; nvs_mmb=; vsm_ddn=; nrexctr=; evt_time=;<br><br>In general, you don't need to include this attribute in reports, since the data is available in a more consumable fashion using other attributes. |
| Timestamp                            | Timestamp of the event in the collector's timezone.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Records Affected                     | Not used. Instead, use the attributes DATA SETS Records Retrieved, Updated, Deleted, Inserted.                                                                                                                                                                                                                                                                                                                                                                                            |
| Returned Data                        | Not used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Full SQL ID                          | Unique, sequenced identifier for this event. Can be helpful for sorting events in sequence.                                                                                                                                                                                                                                                                                                                                                                                               |
| Ack Response Time                    | Microsecond value from Timestamp of the event on the mainframe.<br>Example: 677032<br>It is not recommended to use this field for sorting as it does not include leading zeros. Use Full SQL ID instead.                                                                                                                                                                                                                                                                                  |
| Statement Type                       | Not used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Blind Variables Values               | Not used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| IMS/DATA SET Program Name            | The name of the application program issuing the data set calls or other access.                                                                                                                                                                                                                                                                                                                                                                                                           |
| IMS/DATA SET Step Name               | JCL step name for the executing program.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| IMS/DATA SET Step Number             | JCL step number for the executing program.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| IMS/DATA SET Previous DSN            | Data Set name before the rename occurred.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| IMS/DATA SET Name                    | The data set name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| IMS/DATA SET Context                 | Type of activity. Examples for Data Set level reporting: DATA SET OPEN, DATA SET CLOSE, Member Delete, Member update, Security facility READ violation, Security facility ALTER violation, etc. For record level monitoring: Record Insert, Record Read, Record Update, and Record Delete.                                                                                                                                                                                                |
| IMS SMF/DATA SET Expiration Days     | How many days until the data set expires.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| IMS SMF/DATA SET Expiration IPL Time | Not used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| IMS SMF/DATA SET Type                | Possible values for Data set monitoring: VSAM, Non-VSAM.<br><br>Possible values for record level monitoring: RRDS, KSDS, VRRDS                                                                                                                                                                                                                                                                                                                                                            |
| IMS/DATA SET Job Name                | Job name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| IMS/DATA SET Job Number              | Job number                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| IMS/DATA SET User ID                 | ID of originating request, such as the TSO or RACF authid.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| DATA SET Records                     | Total number of records. Only written on close events. VSAM only.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| DATA SET Records Updated             | Number of records updated in this event. Only written on close events. VSAM only.                                                                                                                                                                                                                                                                                                                                                                                                         |
| DATA SET Records Deleted             | Number of records deleted in this event. Only written on close events. VSAM only.                                                                                                                                                                                                                                                                                                                                                                                                         |
| DATA SET Records Inserted            | Number of record inserted in this event. Only written on close events.. VSAM only                                                                                                                                                                                                                                                                                                                                                                                                         |
| DATA SET Records Retrieved           | Number of records read in this event. Only written on close events. VSAM only.                                                                                                                                                                                                                                                                                                                                                                                                            |
| DATA SET User Group ID               | Security system group ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| VSAM RLM CICS User ID                | Available only if CICS_SUPPORT is enabled for the S-TAP and the CICS system is configured to send the relevant information to the S-TAP as specified in the Guardium S-TAP for Data Sets on z/OS User's Guide.                                                                                                                                                                                                                                                                            |
| VSAM RLM CICS Transaction ID         | Available only if CICS_SUPPORT is enabled for the S-TAP and the CICS system is configured to send the relevant information to the S-TAP as specified in the Guardium S-TAP for Data Sets on z/OS User's Guide.                                                                                                                                                                                                                                                                            |
| VSAM RLM CICS Program ID             | Available only if CICS_SUPPORT is enabled for the S-TAP and the CICS system is configured to send the relevant information to the S-TAP as specified in the Guardium S-TAP for Data Sets on z/OS User's Guide.                                                                                                                                                                                                                                                                            |
| VSAM RLM CICS Terminal ID            | Available only if CICS_SUPPORT is enabled for the S-TAP and the CICS system is configured to send the relevant information to the S-TAP as specified in the Guardium S-TAP for Data Sets on z/OS User's Guide.                                                                                                                                                                                                                                                                            |
| VSAM RLM CICS File ID                | Available only if CICS_SUPPORT is enabled for the S-TAP and the CICS system is configured to send the relevant information to the S-TAP as specified in the Guardium S-TAP for Data Sets on z/OS User's Guide.                                                                                                                                                                                                                                                                            |

| Attribute                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VSAM RLM CICS Region ID         | Available only if CICS_SUPPORT is enabled for the S-TAP and the CICS system is configured to send the relevant information to the S-TAP as specified in the Guardium S-TAP for Data Sets on z/OS User's Guide.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| VSAM RLM CICS Function Code     | Available only if CICS_SUPPORT is enabled for the S-TAP and the CICS system is configured to send the relevant information to the S-TAP as specified in the Guardium S-TAP for Data Sets on z/OS User's Guide. See above. The possible function codes and their mappings are as follows:<br>1 – READ_INTO<br>2 – READ_SET<br>3 – READ_UPDATE_SET<br>4 - READ_UPDATE_INTO<br>5 – WRITE<br>6 – REWRITE<br>8 – REWRITE_DELETE<br>10 – DELETE<br>11 – UNLOCK<br>12 – START_BROWSE<br>13 – READ_NEXT_INTO<br>14 – READ_NEXT_SET<br>15 – READ_PREVIOUS_INTO<br>16 – READ_PREVIOUS_SET<br>17 – READ_NEXT_UPDATE_INTO<br>18 – READ_NEXT_UPDATE_SET<br>19 - READ_PREVIOUS_UPDATE_INTO<br>20 - READ_PREVIOUS_UPDATE_SET<br>21 – RESET_BROWSE<br>22 – END_BROWSE |
| VSAM SMF Access Type            | Possible values: IN, OUT Written only on CLOSE events. Distinguishes whether an access was "open for read" (IN) or "open for update" (OUT).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| IMS/DATA SET Event Time         | Timestamp of the event as recorded on the host in UTC format. The collector timezone is in the Timestamp field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| DATA SET Non-VSAM Member        | If a PDS or PDSE member is allocated and opened, Member name is reported on event close. For programs that can access/update multiple members, such as IEBCOPY, member names are not reported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| DATA SET DD Name                | The data definition (DDNAME) in the JCL or dynamically allocated by the started task.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Data SET Non-VSAM EXCP Count    | The execute channel program (EXCP) counts for non-VSAM data sets, which basically tells you the number of reads and writes against these non-VSAM data sets. This allows for more granular reporting of access to partitioned data sets.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| DATA SET RLM DD Name            | The data definition (DDNAME) in the JCL or dynamically allocated by the started task for RLM monitoring.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Timestamp(microsec)             | Not used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| More information                | Contains CICS Unit of Work ID. There is no reason to use this attribute in your report. Use the DB2 z/IMS/DATA SET attribute for a more consumable version of this information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| DB2 z/IMS/DATA SET Unit of Work | CICS unit of work ID, in hex. Only available for record-level monitoring.<br>0x0000000000000000 if this activity is not part of a CICS transaction and RLM is not activated for a file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| DATA SET Non-VSAM New Member    | If a PDS or PDS/E member name is renamed, this is the new name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

Table 5. Attributes for SQL Entity (Data Sets). The SQL Entity provides no added value for Data Sets reporting. Use the attributes you need from the Full SQL Entity instead

| Attribute     | Description                                                                                                  |
|---------------|--------------------------------------------------------------------------------------------------------------|
| SQL           | Contains a subset of fields from the FULL SQL entity. There is no reason to use this attribute in reporting. |
| Truncated SQL | Not used for data sets.                                                                                      |

Table 6. Attributes for Command Entity (Data Sets)

| Attribute | Description                                                                                                                                                              |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SQL Verb  | The event type. See Data Set Context Field in Full SQL for examples. If this field is added to a report built with Main Entity of Full SQL, this is reported as a count. |

Table 7. Attributes for Object Entity (Data Sets)

| Attribute                 | Description                                              |
|---------------------------|----------------------------------------------------------|
| Object Name               | Name of the data set.                                    |
| Object Type               | Format of the object such as KSDS, RRDS, VSAM, non-VSAM. |
| IMS Segment/DSN/PART/AREA | The data set name.                                       |

Table 8. Attributes for Field Entity (Data Sets)

| Attribute | Description |
|-----------|-------------|
| Field     | Not used.   |

#### Exception Domain

There is no useful information logged in exception domain for Data Sets.

## Built-in reports for DB2 for z/OS

For DB2, there are no built-in reports specifically for z/OS. In many cases, the existing Guardium built-in reports work fine, with perhaps some minor changes because of the way z-specific fields are mapped to the Guardium internal database.

Some of these mappings are shown in the following table.

Table 1. Key mappings of DB2 for z/OS concepts to Guardium report fields

| Concept                                                                                                          | Entity                           | Attribute                           |
|------------------------------------------------------------------------------------------------------------------|----------------------------------|-------------------------------------|
| Subsystem ID                                                                                                     | Client/Server                    | Service Name                        |
| Location Name                                                                                                    | Client/Server                    | Service Description                 |
| Database Name                                                                                                    | Access Period                    | DB2 i/z Database                    |
| Plan Name of originating request                                                                                 | App User Name (or Access Period) | App User Name (or Application User) |
| DBRM name for originating request (For example, SYSLH200 is used to execute JDBC distributed dynamic statements) | Access Period                    | DB2 i/z Program Name                |

Tip: You can rename report columns as you like by going to the Query-Report Builder, access the query, click the Display Options row and modify the column headings.

## Example reports for DB2 for z/OS

This section includes queries that you can use as a base for building your own DB2 for z/OS reports.

Start by looking at the following queries:

- DB2 z/OS Connection Report (Main Entity: Session Start). This report can help you get the “big picture” of what types of applications and users are connecting to your DB2 environment.
- DML on Sensitive Objects (Main Entity: Object) This report depends on two groups: One that contains your sensitive objects and one that contains DML commands. You can easily clone the beginning of this report from the System-defined report “DML Execution on Sensitive Objects” and add the additional columns such as Network Protocol and Service Name.

Table 1. DB2 z/OS Connection Report Query Fields (Main Entity: Session Start)

| Entity        | Attribute        | Field Mode                                                | Comments                                                                                                                                                                                                                                                |
|---------------|------------------|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Session       | Session Start    | Value (Check Order-by, Sort Rank 1 and check Dec end box) |                                                                                                                                                                                                                                                         |
| Client/Server | Service Name     | Value                                                     | This is the SSID                                                                                                                                                                                                                                        |
| Client/Server | DB User Name     | Value                                                     |                                                                                                                                                                                                                                                         |
| Client/Server | Network Protocol | Value                                                     | Concatenation of Connection Name and Connection Type. Example TSO:BATCH and DRDA:SERVER                                                                                                                                                                 |
| Client/Server | Client IP        |                                                           |                                                                                                                                                                                                                                                         |
| Client/Server | Server IP        |                                                           |                                                                                                                                                                                                                                                         |
| Client/Server | Source Program   |                                                           | Concatenation of server name with correlation name and ID. Could vary based on what the application sends. Example from distributed application (DB2JCC) could be: GUARDIUMZ4.SVL.I:DB2JCC_APPL A CICS transaction could be the transaction identifier. |

Table 2. DB2 z/OS Connection Report: Query Conditions

| Entity              | Attribute and Operator                  | Comments                                                             |
|---------------------|-----------------------------------------|----------------------------------------------------------------------|
| WHERE Client/Server | DB Protocol=Value DB2/Z                 | This narrows report to just DB2 z/OS traffic.                        |
| AND Client/Server   | Service Name LIKE Parameter ServiceName | Use % in your runtime parameters to display data from all SSID data. |
| AND Client/Server   | DB User Name LIKE Parameter DBUser      | Use % in your runtime parameters to display all data.                |

Table 3. DML on Sensitive Objects Query Fields (Main Entity: Object)

| Entity        | Attribute        | Field Mode                                                  | Comments                                                                                                                            |
|---------------|------------------|-------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| FULL SQL      | Timestamp        | Value                                                       |                                                                                                                                     |
| Client/Server | Service name     | Value                                                       | This is the SSID.                                                                                                                   |
| Client/Server | Network Protocol | Value                                                       | Concatenation of Connection Name and Connection Type. Example TSO:BATCH and DRDA:SERVER                                             |
| Client/Server | DB User Name     | Value                                                       |                                                                                                                                     |
| Object        | Object Name      | Value                                                       |                                                                                                                                     |
| Command       | SQL Verb         |                                                             |                                                                                                                                     |
| Client/Server | Client IP        |                                                             |                                                                                                                                     |
| FULL SQL      | Full SQL         |                                                             | This field is populated only with LOG FULL DETAILS policy rule.                                                                     |
| FULL SQL      | Full SQL ID      | Value with Order-by checked, Sort-by =1 and Descend checked | This can help order events within a second in the correct order.<br>This field is populated only with LOG FULL DETAILS policy rule. |

| Entity             | Attribute       | Field Mode | Comments                                                                                                                                                                                                                 |
|--------------------|-----------------|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| App User Name      | App User name   | Value      | Consists of PLAN, SQLID, PROG and DB_NAME Example: PLAN=DISTSERV ; SQLID=SYSADM ; PROG=SYSLH200 ; DB_NAME=DSN00006<br><br>Note: If AppEvents mechanism is used to collect 'real' end user, this field will display that. |
| Application Events | DB2 Client Info | Value      | Information in the DB2 Client Info depends on what the application assigns to these fields. None, some, or all values could be populated: WSUSER, APPL, WKSTN.                                                           |

Table 4. DML on Sensitive Objects Query Conditions

| Entity              | Attribute and Operator                                                                             | Comments                                                                                                                                                                                                         |
|---------------------|----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WHERE Client/Server | DB Protocol=Value DB2/Z                                                                            | This narrows report to just DB2 z/OS traffic.                                                                                                                                                                    |
| AND Client/Server   | Service Name LIKE Parameter Service Name                                                           | Use % in your runtime parameters to display data from all SSIDs.                                                                                                                                                 |
| AND Client/Server   | DB User Name LIKE Parameter DB User                                                                | Use % in your run time parameters to display all data                                                                                                                                                            |
| AND Object          | Object Name LIKE GROUP Sensitive Objects (or whatever you have named your sensitive objects group) | Objects could be views, aliases, package names, or plan names. If Quick Parse Native is used, the schema.base-table-name is used instead of view or aliases. Make sure your groups accommodate this flexibility. |
| AND Command         | SQL Verb IN GROUP DML Commands (or whatever you have named your DML group)                         |                                                                                                                                                                                                                  |

Tip: Reporting on **SELECT \* Users**: You can choose whichever query fields you like and include a query condition for Full SQL **LIKE Value %select%\***. Alternatively, you can specify this as a Parameter and specify it at run time (using the wrench icon to customize the run time parameters).

## Report entities and attributes for DB2 for z/OS

Use this information to find reporting attributes for DB2 for z/OS.

This is not meant to be a complete listing of all entities and attributes. See [Domains, Entities, and Attributes](#) for the complete list.

Table 1. Attributes for Client/Server Entity (DB2 for z/OS)

| Attribute          | Description                                                                                                                                                                                                                                              |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Timestamp          | All attributes in this session are static, so this timestamp is created only once, when Guardium observes a request on the defined connection for the first time.                                                                                        |
| OS User            | OS USER, TSO logon ID, or Authid for batch job.<br>Example: SYSADM                                                                                                                                                                                       |
| DB User Name       | Authorization ID                                                                                                                                                                                                                                         |
| Service Name       | DB2 SSID                                                                                                                                                                                                                                                 |
| Server Description | DB2 Location name.<br>Example: STLEC1                                                                                                                                                                                                                    |
| Network Protocol   | Concatenation of connection type and name.<br>Example: TSO:BATCH and DRDA:SERVER                                                                                                                                                                         |
| DB Protocol        | DB2/Z.                                                                                                                                                                                                                                                   |
| Client IP          | This is the IP Address of the client workstation for distributed connections.                                                                                                                                                                            |
| Server Host Name   | LPAR name - example: LABEC247                                                                                                                                                                                                                            |
| Source Program     | Concatenation of Server name with correlation name and ID. Could vary based on what the application sends. Example from distributed application (DB2JCC) could be: GUARDIUMZ4.SVL.I:DB2JCC_APPL. A CICS transaction could be the transaction identifier. |
| Server Type        | DB2. If more than one type of database is writing events to the Guardium system, this field helps separate the events.                                                                                                                                   |

Table 2. Attributes for Session Entity

| Attribute     | Description                                                                                                                                                                                                                                          |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Session Start | Sessions in z/OS are not able to be specified the same way as in distributed platforms, which relies on logins and logouts to the database. A session identifier is based on a set of characteristics and the timestamp recorded for that "session." |
| Session End   | Timestamp recorded after a period of no activity on the associated session.                                                                                                                                                                          |
| UID Chain     | Contains the VTAM network ID. Example: NETWORK_ID=G91E7FCC                                                                                                                                                                                           |
| Terminal ID   | For distributed access, this is the outgoing client port or socket In hex.<br>Example: A314 (port 41748)                                                                                                                                             |
| Process ID    | This is a thread token identifier. You probably won't need this for normal reporting purposes.                                                                                                                                                       |

Table 3. Attributes for Client Server / Session Entity

| Attribute                                                     | Description                                                                                                                                            |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server IP/Port                                                | Server IP concatenate with zero. Server port is always 0.                                                                                              |
| Client IP/Src App/DB User/Server IP/Svc. Name/OS User/DB Name | A tuple containing the named fields. Note: DB Name is always blank. You must obtain DB Name from the Access Period Entity, DB2 i/z Database attribute. |
| UID Chain                                                     | Contains the VTAM network ID.<br>Example: NETWORK_ID=G91E7FCC                                                                                          |
| Terminal ID                                                   | For distributed access, this is the outgoing client port or socket In hex.<br>Example: A314 (port 41748)                                               |
| Process ID                                                    | This is a thread token identifier. You probably won't need this for normal reporting purposes.                                                         |

Table 4. Attributes for Access Period Entity (DB2 for z/OS)

| Attribute | Description |
|-----------|-------------|
|-----------|-------------|

| Attribute             | Description                                                                                                                                                        |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DB2 i/z Program       | This is the name of the DBRM that contains the executable code within the bound plan.<br>Example: SYS1H200 is used to execute JDBC distributed dynamic statements. |
| DB2 i/z Database      | Database name<br>Example: DSN00006                                                                                                                                 |
| Application User Name | This consists of consists of PLAN, SQLID, PROG and DB_NAME Example: PLAN=DISTSERV ; SQLID=SADM ; PROG=SYS1H200 ; DB_NAME=DSN00006                                  |
| SQL                   | SQL text “template”; i.e., construct. Field values are replaced by question marks.<br>Example: INSERT INTO GDMC_LABEC247_VA1A VALUES (?, ?, ?, ?, ?, ?, ?)         |

Table 5. Attributes for Full SQL Entity (DB2 for z/OS)

| Attribute                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ID                                        | A generated value for each statement. You can use this to put statements in order.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Timestamp                                 | A timestamp from the DB2 server.<br>Example: 2012-04-25-11.51.40.005951                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Ack Response Time                         | Microsecond value from Timestamp.<br>Example: 677032<br>It is not recommended to use this field for sorting as it does not include leading zeros. Use FullSQL ID instead.                                                                                                                                                                                                                                                                                                                                                               |
| Records Affected                          | Number of rows, valid for SELECT, INSERT, or DELETE. -1 if not applicable or if number of rows is not available.                                                                                                                                                                                                                                                                                                                                                                                                                        |
| More Information: TSSTOC=; stmttyp=; pds= | This contains a variety of information.<br><br>TSSTOC=. Store clock value. Example: TSSTOC=0x00D13309E22C45D8D4000000012F0001; May be useful to facilitate correlation of events within a commit or rollback.<br><br>Stmttyp= 'S' for Static and 'D' for Dynamic. If you want to sort by this field, then it's recommended that you use the DB2 z Statement Type attribute of this Entity instead, which pulls this value into a separate attribute.<br><br>pds- For a Bind Package command, this is the PDS Name for the DBRM members. |
| Bind Variables Values                     | The values of the host variables. To log masked data instead, use LOG MASKED DETAILS policy rule for the appliance.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Full SQL                                  | Full SQL statement logged for each occurrence. Example: INSERT INTO GDMC_LABEC247_VA1A VALUES ('/08/15/16 19:49:56.653', '/08/15/16 19:49:56.653'--, 1, 1, 1, 'guardiumz4 -count -update -server nulldn9seq -test_duration 7 -delay 999 -concurrent_connections 1')<br><br>This can also contain the full BIND PLAN and BIND PACKAGE commands.<br><br>Note: Values can be masked by using LOG MASKED DETAILS in the appliance policy.                                                                                                   |
| App User Name                             | Displays the user name from the App Event entity of an App Event exists; otherwise, displays Application User from Access Period Entity.                                                                                                                                                                                                                                                                                                                                                                                                |
| DB2 z/IMS/DATA SET Unit of Work           | Computed attribute containing the CICS Unit of Work ID that can be used to correlate CICS traffic across multiple S-TAP Entities (IMS, Data Sets, and DB2).                                                                                                                                                                                                                                                                                                                                                                             |
| DB2 z Statement Type                      | Computed attribute that contains either 'Static' or 'Dynamic'.                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| DB2 z/IMS/DATA SET Unit of Work           | CICS unit of work ID, in hex. Can be used to correlate data access events across DB2, IMS and Data Sets within a CICS Transaction.<br><br>This field is blank if this activity is not part of a CICS transaction.                                                                                                                                                                                                                                                                                                                       |

Note: The appliance-side policy for DB2 for z/OS activities must include the logging action LOG FULL DETAILS to collect Full SQL data. Otherwise, you will only get data in the SQL Entity attributes.

Table 6. Attributes for Application Events Entity (DB2 for z/OS)

| Attribute       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DB2 Client Info | Information in the DB2 Client Info depends on what the application assigns to these fields. None, some, or all values could be populated:<br><br>WSUSER= The user ID of the client end user. Can be CICS original signon client, if used.<br><br>APPL= The application or transaction name of the end user's application.<br><br>WKSTN= The workstation name of the client end user.<br><br>The following two fields are populated only when z/OS Identity propagation is used: DN=X.500 distinguished name<br><br>REG=X.500 registry name<br><br>Example: WSUSER=SYSADM;WRKSTN=guardiumz4.svl.ibm;APPL=db2jcc_application;DN=;REG= |

Table 7. Attributes for SQL Entity (DB2 for z/OS)

| Attribute     | Description                                                                                                                                                                                                                                               |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SQL           | SQL text by construct. Constructs only reflect the SQL template text and will not log each instance that a matching statement is executed, only once per hour (reporting period).<br>Example: INSERT INTO GDMC_LABEC247_VA1A VALUES (?, ?, ?, ?, ?, ?, ?) |
| Truncated SQL | Yes or No. This is historical and is not used any more.                                                                                                                                                                                                   |

Table 8. Attributes for Command Entity

| Attribute | Description                                                                                                                                                                                                                                                                                                                 |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SQL Verb  | This is the SQL verb, such as SELECT, INSERT, UPDATE, DELETE, BIND PLAN or BIND PACKAGE.<br><br>Prior to 10.1.3, the SQL Verb would be recorded differently when Quick Parse Native is used (TABLE READ or TABLE WRITE). With 10.1.3, the Verb will more closely match what is used when LOG FULL DETAILS or ALLOW is used. |

Note: SQL Verb will only be a count in a report created with a Full SQL main entity.

Table 9. Attributes for Object Entity (DB2 for z/OS)

| Attribute   | Description                                                                                                                                                                                                                                                               |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Object Name | This is the object used in the SQL, such as the table, view, alias name, plan name, package name, bind plan owner.<br><br>However, if the policy uses a Quick Parse Native action, then a data object will always be the base table in the format schema-name.table-name. |

Table 10. Attributes for Field Entity (DB2 for z/OS)

| Attribute  | Description                                                                                                                                                                                                                              |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Field Name | This is the column name used in the SQL.<br>Note: You will get field names in other Entities (SQL or Full SQL); this Entity is used for reporting on lists of fields. Use of Quick Parse Native will not allow population of this field. |

Table 11. Attributes for the Exception Entity  
(Main entity: Exception) (DB2 for z/OS)

| Attribute             | Description                          |
|-----------------------|--------------------------------------|
| Exception Description | Contains the negative SQLCODE.       |
| Database Error Text   | The text associated with this error. |

Attention:

- With z/OS, you must specify on the Collection Profile policy rule that you want to collect negative SQLCODEs, and you must also specify which codes to collect. See the following table for a list of negative SQL codes that you might find useful. Refer to the Knowledge Center documentation for DB2 for z/OS to see the complete list of codes to tailor the list to your own needs.
- Some negative SQL codes support descriptions with real SQL values. Where available, these descriptions are included in the "SQL string that caused the exception" report column. Take for example the base description of SQLCODE -556:

```
revoke-target CANNOT HAVE THE privilege PRIVILEGE object-name REVOKED BY revoker-id
BECAUSE THE REVOKEE DOES NOT POSSESS THE PRIVILEGE OR THE REVOKER DID NOT MAKE THE GRANT
```

This description can be presented with real values:

```
ADMF002 CANNOT HAVE THE SELECT PRIVILEGE ON SYSADM.HOLLK REVOKED BY ADMF001
BECAUSE THE REVOKEE DOES NOT POSSESS THE PRIVILEGE OR THE REVOKER DID NOT MAKE THE GRANT
```

Table 12. Suggested list of negative SQL Codes to audit

|        | Description                                                                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -164   | authorization-id DOES NOT HAVE THE PRIVILEGE TO CREATE A VIEW WITH QUALIFICATION qualifier-name                                                                                                                             |
| -204   | name IS AN UNDEFINED NAME                                                                                                                                                                                                   |
| -206   | object-name IS NOT VALID IN THE CONTEXT WHERE IT IS USED                                                                                                                                                                    |
| -551   | auth-id DOES NOT HAVE THE PRIVILEGE TO PERFORM OPERATION operation ON OBJECT object-name                                                                                                                                    |
| -552   | authorization-id DOES NOT HAVE THE PRIVILEGE TO PERFORM OPERATION operation                                                                                                                                                 |
| -553   | AUTHORIZATION ID OR SCHEMA NAME name SPECIFIED IS NOT VALID FOR REQUESTED OPERATION                                                                                                                                         |
| -554   | AN AUTHORIZATION ID OR ROLE CANNOT GRANT A PRIVILEGE TO ITSELF                                                                                                                                                              |
| -555   | AN AUTHORIZATION ID OR ROLE CANNOT REVOKE A PRIVILEGE FROM ITSELF                                                                                                                                                           |
| -556   | revoke-target CANNOT HAVE THE privilege PRIVILEGE object-name REVOKED BY revoker-id BECAUSE THE REVOKEE DOES NOT POSSESS THE PRIVILEGE OR THE REVOKER DID NOT MAKE THE GRANT                                                |
| -557   | INCONSISTENT GRANT/REVOKE KEYWORD keyword. PERMITTED KEYWORDS ARE keyword-list                                                                                                                                              |
| -559   | ALL AUTHORIZATION FUNCTIONS HAVE BEEN DISABLED                                                                                                                                                                              |
| -562   | THE SPECIFIED PRIVILEGES CANNOT BE GRANTED TO PUBLIC.                                                                                                                                                                       |
| -567   | bind-type AUTHORIZATION ERROR USING auth-id AUTHORITY PACKAGE = package-name PRIVILEGE = privilege                                                                                                                          |
| -592   | NOT AUTHORIZED TO CREATE FUNCTIONS OR PROCEDURES IN WLM ENVIRONMENT env-name                                                                                                                                                |
| -807   | ACCESS DENIED: PACKAGE package-name IS NOT ENABLED FOR ACCESS FROM connection-type connection-name                                                                                                                          |
| -908   | bind-type ERROR USING auth-id AUTHORITY. BIND, REBIND OR AUTO-REBIND OPERATION IS NOT ALLOWED                                                                                                                               |
| -922   | AUTHORIZATION FAILURE: error-type ERROR. REASON reason-code                                                                                                                                                                 |
| -20264 | FOR TABLE table-name, primary-auth-id WITH SECURITY LABEL primary-auth-id-seclabel IS NOT AUTHORIZED TO PERFORM operation ON A ROW WITH SECURITY LABEL row-seclabel. THE RECORD IDENTIFIER (RID) OF THIS ROW IS rid-number. |
| -20361 | AUTHORIZATION ID authorization-name IS NOT DEFINED FOR THE TRUSTED CONTEXT context-name                                                                                                                                     |
| -20372 | THE SYSTEM AUTHID CLAUSE OF A CREATE OR ALTER TRUSTED CONTEXT STATEMENT FOR context-name SPECIFIED authorization-name, BUT ANOTHER TRUSTED CONTEXT IS ALREADY DEFINED FOR THAT AUTHORIZATION ID.                            |
| -20373 | A CREATE OR ALTER TRUSTED CONTEXT STATEMENT SPECIFIED authorization-name MORE THAN ONCE OR THE TRUSTED CONTEXT IS ALREADY DEFINED TO BE USED BY THIS AUTHORIZATION ID, PROFILE NAME, OR PUBLIC.                             |
| -20374 | AN ALTER TRUSTED CONTEXT STATEMENT FOR context-name SPECIFIED authorization-name BUT THE TRUSTED CONTEXT IS NOT CURRENTLY DEFINED TO BE USED BY THIS AUTHORIZATION ID, PROFILE NAME, OR PUBLIC                              |
| -30053 | OWNER AUTHORIZATION FAILURE                                                                                                                                                                                                 |
| -30060 | RDB AUTHORIZATION FAILURE                                                                                                                                                                                                   |

## Built-in reports for IMS

### IMS Checkpoint Results

This is not a report you would use for auditing. This IMS S-TAP report is used internally to track information. You cannot modify or clone this report.

### IMS Access

This report provides an overview of access (a profile) within the default 1 hour reporting periods. Note that you should change the runtime parameter of DB Protocol and/or Server Type to narrow results to IMS.

### IMS Data Access Details

Uses the full SQL Entity as the main entity and provides full details of each access to IMS.

Tip: When you clone this report, optionally add the DB Protocol attribute from Client/Server as a query condition to avoid mixing this report with other information that may be sent to this appliance.

#### IMS Event

A good report for summarizing the type of access (such as DLI), the psb\_name, and the command and object mapping.

Tip: When you clone the IMS Event report, remove DB User Name from both the column and query condition and replace it with the IMS/DATA SET User ID attribute under the Full SQL entity. In addition, add the Full SQL ID as the last column of the report so you use it for sorting and more clearly see a sequence of events for forensics, as the regular timestamp may not provide enough precision.

You can modify the column names to be more reflective of the content, such as changing Application User to PSB Name.

#### IMS Object

This report provides an object-level view of access.

Tip: When you clone this report, make the following modifications:

- Remove DB User Name from both the column and query condition and replace it with the IMS/DATA SET User ID attribute under the Full SQL entity.
- Remove the Object Type field as well, as this is not populated.
- Add the Full SQL ID as a column as the last column of the report to more clearly see a sequence of events for forensics

## Example reports for IMS

This section includes queries that you can use as a base for building your own IMS reports.

Note: Performance on the reports will be slower the more runtime parameters using 'LIKE' that you add. If you are sending out regularly scheduled batch reports, consider using more hard coded parameters for the query conditions.

The query in the following table is very similar to the IMS Data Detail built in report, but it narrows results to just DLI and also includes some additional fields such as IMS Terminal, IMS Segment, and the SSID (Service Name).

Table 1. IMS DLI Detail Report Query Fields (Main entity: FULL SQL)

| Entity        | Attribute            | Field Mode                                                       | Comments                                                                             |
|---------------|----------------------|------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| FULL SQL      | Timestamp            | Value                                                            |                                                                                      |
| Client/Server | Service Name         | Value                                                            | SSID as defined in the Guardium IMS Definitions panel.                               |
| Client/Server | Server Type          | Value                                                            | Example: IMS                                                                         |
| FULL SQL      | MS/DATA SET User ID  | Value                                                            |                                                                                      |
| Client/Server | Network Protocol     | Value                                                            |                                                                                      |
| FULL SQL      | Source Program       | Value                                                            |                                                                                      |
| FULL SQL      | IMS Transaction      | Value                                                            |                                                                                      |
| FULL SQL      | IMS Terminal         | Value                                                            |                                                                                      |
| FULL SQL      | IMS Segment          | Value                                                            |                                                                                      |
| FULL SQL      | Bind Variable Values | Value                                                            |                                                                                      |
| FULL SQL      | Full SQL             | Value                                                            |                                                                                      |
| FULL SQL      | Full SQL ID          | Value. Order by is checked, sort rank 1, and Descend is checked. | This helps to sequence events in a report when the timestamp is not granular enough. |

Table 2. IMS DLI Detail Report Query Conditions

| Entity            | Attribute and Operator                       | Comments                                                                                         |
|-------------------|----------------------------------------------|--------------------------------------------------------------------------------------------------|
| Client/Server     | Server Type LIKE Value IMS                   |                                                                                                  |
| AND Client/Server | Network Protocol LIKE Value DLI              |                                                                                                  |
| AND Client/Server | Service Name LIKE Parameter ServiceName      |                                                                                                  |
| AND FULL SQL      | IMS/DATASET User ID LIKE Parameter IMSUserID | At runtime, use % or specify a user ID or wildcarded user ID.                                    |
| AND FULL SQL      | Full SQL LIKE Parameter FULLSQL              | At runtime, use % or specify a wild card for a portion of the full SQL string.<br>Example: %GET% |

Table 3. Query for IMS Privileged User Report Query Fields (Main entity: FULL SQL)

| Entity        | Attribute                 | Field Mode | Comments                                               |
|---------------|---------------------------|------------|--------------------------------------------------------|
| FULL SQL      | Timestamp                 | Value      |                                                        |
| Client/Server | Service Name              | Value      | SSID as defined in the Guardium IMS Definitions panel. |
| Client/Server | Server Type               | Value      | Example: IMS                                           |
| Full SQL      | IMS/DATA SET User ID      | Value      |                                                        |
| Client/Server | Network Protocol          | Value      |                                                        |
| FULL SQL      | IMS/DATA SET Program Name | Value      |                                                        |
| FULL SQL      | DBD                       | Value      |                                                        |
| FULL SQL      | IMS/DATA SET Context      | Value      |                                                        |
| FULL SQL      | IMS/DATA SET Job Name     | Value      |                                                        |
| FULL SQL      | IMS/DATA SET Job Number   | Value      |                                                        |
| Access Period | IMS PSB NAME              | Value      |                                                        |
| FULL SQL      | IMS Segment               | Value      |                                                        |

| Entity        | Attribute           | Field Mode                                                       | Comments                                                                                                                                                                                 |
|---------------|---------------------|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FULL SQL      | IMS PCB NAME        | Value                                                            |                                                                                                                                                                                          |
| FULL SQL      | IMS Transaction     | Value                                                            |                                                                                                                                                                                          |
| FULL SQL      | IMS Terminal        | Value                                                            |                                                                                                                                                                                          |
| FULL SQL      | IMS DLI Status Code | Value                                                            | If you collected audit events that have non-blank status codes, this field will contain those. Non-blank status codes can indicate that the DLI call failed or completed with a warning. |
| Client/Server | Client IP           | Value                                                            |                                                                                                                                                                                          |
| Client/Server | Server IP           | Value                                                            |                                                                                                                                                                                          |
| FULL SQL      | Full SQL ID         | Value. Order by is checked, sort rank 1, and Descend is checked. | This helps to sequence events in a report when the timestamp is not granular enough.                                                                                                     |
| FULL SQL      | Full SQL            | Value                                                            |                                                                                                                                                                                          |

Table 4. Query for IMS Privileged User Report Query Conditions

| Entity              | Attribute and Operator                       | Comments                                                                                                                                                                                                                                                                                     |
|---------------------|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WHERE Client/Server | Network Protocol LIKE Value DLI              | Make this a runtime parameter instead if you are concerned with privileged activity related to activities reported by SMF and IMS Log reporting.                                                                                                                                             |
| AND Client/Server   | Service Name LIKE Parameter ServiceName      | SSID as defined in the Guardium IMS Definitions panel.                                                                                                                                                                                                                                       |
| AND FULL SQL        | IMS/DATASET User ID LIKE Parameter IMSUserID |                                                                                                                                                                                                                                                                                              |
| AND FULL SQL        | Full SQL LIKE Parameter FULLSQL              | At runtime, use % or specify a wild card for a portion of the full SQL string.<br>Example: %GET%                                                                                                                                                                                             |
| AND FULL SQL        | IMS/DATA SET User ID IN GROUP AdminUserGroup | Use your own group here for where you keep privileged user IDs. This group can be maintained manually, but it more maintainable by regularly scheduling uploads from the external source that maintains these IDs.<br><br>Wild cards are not allowed in this field because of the use of IN. |

## Report entities and attributes for IMS

Use this information to find reporting attributes for IMS.

Table 1. Attributes for Client/Server Entity (IMS)

| Attribute           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Timestamp           | All attributes in this session are static, so this timestamp is created only once, when Guardium observes a request on the defined connection for the first time.                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Service Description | IMS Subsystem ID                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Server Type         | IMS. If more than one type of database is writing events to the Guardium system, this field helps separate the events                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Client IP           | IP address of LPAR . Usually the same as the server IP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Server IP           | IP Address of LPAR.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Network Protocol    | Reflects each type of IMS S-TAP Audit Event collection component: <ul style="list-style-type: none"> <li>DLI- online or batch DL/I activity</li> <li>SMF- data from SMF Data Collector activity monitor, which can collect events on data sets related to IMS.</li> <li>IMS_LOG – data from the IMS Archived Log Data Collector, used to collect events such as IMS user signon and signoff, changes to DBD and PSB status and IMS online region stops and starts</li> <li>IMS_MIS_LOG – data collected from the IMS Missing Log Utility, which analyzes IMS RECON data sets to confirm existence of log data sets.</li> </ul> |
| DB Protocol         | IMS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| DB User Name        | Not populated here for IMS. Use IMS/DATA SET User ID from the FULL SQL entity instead.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Server Host Name    | Hostname of LPAR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Source Program      | Region type of the access. For batch: 'DLI BTC' 'DBB BTC' . For online: MPP (Message processing region), JMP (Java Message Processing), BMP (Batch message processing-Transaction oriented) JBP (Java Batch Processing). Other possible values: AER (Application Execution Region), IFP (IMS Fast Path)                                                                                                                                                                                                                                                                                                                        |
| Service Name        | Subsystem name from IMS Definitions panel. If more than one IMS is being audited, Service Name sorting or filtering allows reporting by IMS system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| OS User             | Not used for IMS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Table 2. Attributes for Session Entity (IMS)

| Attribute  | Description                                                                                                                                                                           |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Timestamp  | Initially, a timestamp created for the first request on a connection. Later, it is updated when it is marked inactive following an extended period of time with no observed activity. |
| Session ID | Unique identifier generated by Guardium. Because IMS does not have the concept of 'sessions', this is not particularly meaningful in IMS reporting.                                   |
| Access ID  | Uniquely identifies the access period                                                                                                                                                 |

Table 3. Attributes for Access Period Entity (IMS)

| Attribute              | Description                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Application User       | IMS Program Specification Block (PSB). Appears as psb_name=name. Use the IMS PSB Name attribute instead to report on the name alone. |
| Failed SQLs            | Not used.                                                                                                                            |
| Total records affected | Not used. -1                                                                                                                         |
| Successful SQLs        | Not applicable for IMS.                                                                                                              |
| IMS PSB Name           | IMS Program Specification Block (PSB)                                                                                                |

| Attribute             | Description                  |
|-----------------------|------------------------------|
| Timestamps (microsec) | Not used. Always contains 0. |

Table 4. Attributes for Full SQL Entity (IMS)

| Attribute                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Full SQL                             | Contains all information about an event. Computed attributes for other report fields are created from this data, which includes:<br>uid=; prog=; job=; step=; tran=; job#=; term=; pcb=; pcb#; dli_sts=; before=; desc=; dbd=; seg=;                                                                                                                                                                                                                             |
| Timestamp                            | Timestamp of the event in the collector's timezone.                                                                                                                                                                                                                                                                                                                                                                                                              |
| Records Affected                     | Not used for IMS. Always -1.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Returned Data                        | Segment data, in hex, as returned to the application.<br>Enabling the return of this data requires the assistance of IBM support to enable the correct policy action. This option is almost never recommended because it means that potentially sensitive data is stored on the collector.                                                                                                                                                                       |
| Full SQL ID                          | Unique, sequenced identifier for this event. Can be helpful for sorting events in sequence.                                                                                                                                                                                                                                                                                                                                                                      |
| Ack Response Time                    | Microsecond value from Timestamp on the event from the mainframe.<br>Example: 677032<br>It is not recommended to use this field for sorting as it does not include leading zeros; use FullSQL ID instead.                                                                                                                                                                                                                                                        |
| Statement Type                       | Not used for IMS. Always contains 'SQL'                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Blind Variables Values               | This is the same as the fieldDB2 z/IMS/DATA SET Unit of Work, prefixed with the SSID. To correlate unit of work IDs across subsystems, it is recommended to use the DB2 z/IMS/DATA SET Unit of Work field instead of this one.                                                                                                                                                                                                                                   |
| IMS/DATA SET Program Name            | The name of the application program issuing the DLI calls or other access.                                                                                                                                                                                                                                                                                                                                                                                       |
| IMS/DATA SET Step Name               | JCL step name for the executing program.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| IMS/DATA SET Step Number             | JCL step number for the executing program.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| IMS Transaction                      | IMS transaction identifier                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| IMS Terminal                         | Terminal ID of the originating request.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| IMS PCB Name                         | The name of the IMS Program Communications Block (PCB)                                                                                                                                                                                                                                                                                                                                                                                                           |
| IMS PCB Number                       | The PCB in the PSB that the program used to access the database                                                                                                                                                                                                                                                                                                                                                                                                  |
| IMS/DATA SET                         | Data set name before an SMF rename.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Previous DSN                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| IMS Database                         | IMS database descriptor (DBD)                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| IMS Segment                          | IMS Segment name in the database.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| IMS/DATA SET Name                    | When SMF is used, the IMS Data Set name that was accessed.                                                                                                                                                                                                                                                                                                                                                                                                       |
| IMS/DATA SET Context                 | Type of activity (such as IMS Segment level GET)                                                                                                                                                                                                                                                                                                                                                                                                                 |
| IMS SMF/DATA SET Expiration Days     | SMF data has expired due to data sitting in the spill file for this number of days. There could be incomplete data. This should be a rare event.                                                                                                                                                                                                                                                                                                                 |
| IMS SMF/DATA SET Expiration IPL Time | SMF data has expired due to an IPL occurring on the host. This could indicate incomplete data.                                                                                                                                                                                                                                                                                                                                                                   |
| IMS Segment Data Length              | The length of the IMS data segment.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| IMS/DATA SET Type                    | The type of data set such as database, image copy, log type, LDS type, recon, and unknown. Applicable only when SMF data collection is used.                                                                                                                                                                                                                                                                                                                     |
| IMS/DATA SET Job Name                | Job name                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| IMS/DATA SET Job Number              | Job number                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| IMS/DATA SET User ID                 | ID of originating request, such as the TSO or RACF authid.                                                                                                                                                                                                                                                                                                                                                                                                       |
| IMS PART/AREA                        | The name of the partition or area. A DEDB can use multiple data sets, called areas, with each area containing the entire data structure. A partition is a subset of a high availability large database (HALDB).                                                                                                                                                                                                                                                  |
| IMS/DATA SET Event Time              | Timestamp of the event as recorded on the host in UTC format.<br><br>The collector timezone is in the Timestamp field.                                                                                                                                                                                                                                                                                                                                           |
| IMS DLI Status Code                  | Status code from DLI. 'bb' means blank (no status code). This is available only when status code collection is specified in the IMS Collection Profile policy as described in<br><a href="https://www.ibm.com/support/knowledgecenter/SSMPHH_10.1.0/com.ibm.guardium.doc.zos/db2_stap_ims/AUI/V1013_AUI/DITA/auuir009.html">https://www.ibm.com/support/knowledgecenter/SSMPHH_10.1.0/com.ibm.guardium.doc.zos/db2_stap_ims/AUI/V1013_AUI/DITA/auuir009.html</a> |
| Timestamp(microsec)                  | Not used.                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| DB2 z/IMS/DATA SET Unit of Work      | Unit of work ID (recovery token), in hex. When the token is from a CICS transaction, it can be used to correlate data access across DB2, IMS and Data Sets within a transaction. (Unlike Data Sets, this token is included even for non-CICS transactions).                                                                                                                                                                                                      |

Table 5. Attributes for SQL Entity (IMS)

| Attribute     | Description                                                  |
|---------------|--------------------------------------------------------------|
| SQL           | Event type (desc=), DBD name (dbd=), and segment name (seg=) |
| Truncated SQL | Not used for IMS.                                            |

Table 6. Attributes for Command Entity (IMS)

| Attribute | Description |
|-----------|-------------|
|-----------|-------------|

| Attribute | Description                                                                                                                   |
|-----------|-------------------------------------------------------------------------------------------------------------------------------|
| SQL Verb  | The event type, which depends on what is collected from the policy.<br>Example: Segment Level GET, REPLACE, INSERT and DELETE |

Table 7. Attributes for Object Entity (IMS)

| Attribute                 | Description                                                                                         |
|---------------------------|-----------------------------------------------------------------------------------------------------|
| Object Name               | DBD name and segment name separated by a colon.                                                     |
| Object Type               | For SMF, the type of data set such as database, image copy, log type, LDS type, recon, and unknown. |
| IMS Segment/DSN/PART/AREA | Name of the segment, data set name (if SMF) partition name, or area.                                |

Table 8. Attribute for Field Entity (IMS)

| Attribute | Description      |
|-----------|------------------|
| Field     | Not used for IMS |

#### Exception Domain

There is no useful information logged in exception domain for IMS. You can collect events that receive particular status codes, but those are reported in the FULL SQL domain (IMS DLI Status Code attribute).

## Assess and harden

The Guardium® Vulnerability Assessment solution is the first step in the security and compliance lifecycle management for any IT environment. You can create a security assessment scan and workflow audits to identify and detect database vulnerabilities in an automated fashion—proactively improving configurations and hardening infrastructures.

- [\*\*Introducing Guardium Vulnerability Assessment\*\*](#)

Guardium Vulnerability Assessment enables you to identify and correct security vulnerabilities in your database infrastructure.

- [\*\*Set up your environment for Vulnerability Assessment\*\*](#)

Set up your central manager and managed units for Vulnerability Assessment.

- [\*\*Types of Vulnerability Assessments\*\*](#)

Guardium provides over two thousand predefined tests to check database configuration parameters, privileges, and other vulnerabilities. Some tests can also be customized to meet specific requirements.

- [\*\*Assessments\*\*](#)

Assessments are a group of tests that scan database infrastructures for vulnerabilities and provide an evaluation of database and data security health with real-time and historical measurements.

- [\*\*IBM Guardium Data Protection app in ServiceNow\*\*](#)

You can configure IBM Security Guardium to track incidents, problems, and tasks discovered by Guardium using the external ticketing system ServiceNow®.

- [\*\*Required schema change\*\*](#)

The schema used by vulnerability assessment tests on IBM Db2® for z/OS® changed in Guardium V9.1. If you upgrade from a release prior to 9.1, you must update your database in order to continue using these tests.

- [\*\*Assessing RACF vulnerabilities\*\*](#)

If you use IBM Db2 for z/OS, you can use vulnerability assessment tests to assess your RACF vulnerabilities. You must have at least version 9.1 of Guardium installed to use RACF assessments.

- [\*\*Configuration Auditing System \(CAS\)\*\*](#)

The Configuration Auditing System (CAS) tracks and reports changes to the server environment; for example, modified configuration files, environment or registry variables, or other database or operating system components. Auditing includes executable files or scripts that are used by the database management system or the operating system. The data is available on the Guardium system and can be used for reports and alerts.

- [\*\*License information for Guardium Vulnerability Assessment\*\*](#)

The license information describes the purchase options for Guardium Vulnerability Assessment. It also describes how to measure the license for Guardium Vulnerability Assessment and perform scans on nonproduction, failover, disaster recovery, and other environments.

## Introducing Guardium Vulnerability Assessment

Guardium Vulnerability Assessment enables you to identify and correct security vulnerabilities in your database infrastructure.

Database Vulnerability Assessment is used to scan the database infrastructure for vulnerabilities and provide evaluation of database and data security health, with real time and historical measurements.

Vulnerability Assessment uses three types of artifacts:

Test

A test checks the database environment for vulnerabilities for a particular threat or area of concern.

Assessment

An assessment is a job that includes a set of tests that are run together.

Data source

The source of data itself, such as a database or XML file, and the connection information necessary for accessing the data.

The Guardium® Vulnerability Assessment application enables organizations to identify and address database vulnerabilities in a consistent and automated fashion. Guardium's assessment process evaluates the health of your database environment and recommends improvement by:

- Assessing system configuration against best practices and finding vulnerabilities or potential threats to database resources, including configuration and behavioral risks. For example, identifying all default accounts that haven't been disabled; checking public privileges and authentication methods chosen, etc.
- Finding any inherent vulnerabilities present in the IT environment, like missing security patches.

- Recommending and prioritizing an action plan based on discovered areas of most critical risks and vulnerabilities. The generation of reports and recommendations provide guidelines on how to meet compliance changes and elevate security of the evaluated database environment.

Guardium's Database Vulnerability Assessment combines two essential testing methods to guarantee full depth and breadth of coverage. It leverages multiple sources of information to compile a full picture of the security health of the database and data environment.

1. Agent-based-Using software installed on each endpoint (e.g. database server). They can determine aspects of the endpoint that cannot be determined remotely, such as administrator's access to sensitive data directly from the database console.
2. Scanning-Interrogating an endpoint over the network through credentialled access.

Included in the Guardium Vulnerability and Threat Management solution are:

- Database Auto-Discovery performs a network auto-discovery of the database environment and creates graphical representation of interactions among database clients and servers.
- Database Content Classifier automatically discovers and classifies sensitive data, such as 16-digit credit card numbers and 9-digit Social Security numbers—helping organizations quickly identify faulty business or IT processes that store confidential data.
- Database Vulnerability Assessment scans the database infrastructure for vulnerabilities and provides evaluation of database and data security health, with real time and historical measurements.
- CAS (Configuration Auditing System) tracks all changes to items such as database structures, security and access controls, critical data values, and database configuration files.
- Compliance Workflow Automation automates the entire compliance process through starting with assessment and hardening, activity monitoring to audit reporting, report distribution, and sign-off by key stakeholders.

CAS (Configuration Auditing System) plays an important role in the identification of vulnerabilities and threats. Guardium pre-configured and user-defined CAS templates can be used in the Assessment test and bring a holistic view of the customer's database environment; With CAS, Guardium can identify vulnerabilities to the database in the OS level such as file permissions, ownership and environment variables. These tests can be seen through the CAS Template Set Definition panel and have the word Assessment in their name.

Note: Configuration Auditing System (CAS) is only supported in English.

Common Vulnerabilities and Exposures (CVE®) is a dictionary of common names (i.e., CVE Identifiers) for publicly known information security vulnerabilities. CVE's common identifiers makes it easier to share data across separate network security databases and tools, and provide a baseline for evaluating coverage such that, if a report incorporates CVE Identifiers, users may quickly and accurately access fix information in one or more separate CVE-compatible databases to remediate the problem.

Numerous organizations have made their information security products and services CVE compatible by incorporating CVE Identifiers. Guardium constantly monitors the common vulnerabilities and exposures (CVE) from the MITRE Corporation and adds these tests for the relevant database related vulnerabilities.

To aid in the finding of individual vulnerabilities while viewing the CVE names for specific databases, the user, when configuring tests through Security Assessment Builder, can select the CVE radio button for the desired database and then select and add the appropriate CVE identifier. Additional information can always be found on the master copy of the CVE list maintained by the MITRE Corporation.

To keep CVEs current within the Guardium solution, Guardium will download and use the most current CVE database to populate a database table with all current CVE entries and candidates. Guardium programmatically compares the downloaded CVE data with the CVE data already in the Guardium Vulnerability Assessment repository; producing a list of new CVEs for review. Guardium Database Security Team then manually reviews these candidates for the Guardium Vulnerability Knowledgebase, tests them and adds the relevant ones to the GA Guardium Vulnerability Assessment Knowledgebase. These tests are tagged with the appropriate CVE number, and once in the GA repository, these tests can automatically run using the Guardium Vulnerability Assessment application.

Note:

- For both Vulnerability Assessments and Entitlements Reporting, when looking for scripts to grant privileges for entitlement reporting, use scripts in the gdmonitor\_scripts directory. Do not use the entitlement\_monitor\_role folder, which is no longer updated.
- When using an expiring product license key, or license with a limited number of datasources, the following message may appear: Cannot add datasource. The maximum number of datasources allowed by license has been reached. The License valid until date and Number of datasources can be seen on the System Configuration panel of the Administrator Console. A Vulnerability or Classification process with N datasources are counted as N scans every time they run.
- Guardium Vulnerability Assessments requires access to the databases it evaluates. To do this, Guardium provides a set of SQL scripts (one script for each database type) that creates users and roles in the database to be used by Guardium.

The template scripts are available on the Guardium system once it is built and can be found and downloaded via fileserver at the following path: /log/debug-logs/gdmonitor\_scripts/. More information is available in the README.txt file.

## Guardium Vulnerability Assessment Test Exceptions

---

The Guardium vulnerability assessment test exception groups are prepopulated with the default members, schema, objects, or privileges created when a database is installed. Use these groups to avoid false-positives when running vulnerability assessments. If an assessment fails, link the appropriate exception group to the test to exclude the default members and run the test again: if the test now runs without violations, this indicates that the initial violations were due to the default members, schema, objects, or privileges created when the database was installed.

For more information, see [Test Exceptions](#).

## MongoDB

---

Developed in 2007, MongoDB is a NoSQL, document-oriented database. MongoDB uses JSON documents with dynamic schemas (this format is called BSON). In MongoDB, a collection is the equivalent of a RDBMS table while documents are equivalent to records in an RDBMS table.

MongoDB is the largest and fastest growing NoSQL database system. It tends to be used as an operational system and as a backend for web applications due to an ease of programming for non-relationally formatted data like JSON documents which are often found in web applications.

- First NoSQL database supported for Guardium Vulnerability Assessment (VA).
- First non-JDBC database connection. Connection uses a Java driver.
- MongoDB data sources support SSL server and client/server connections with SSL client certificates.
- Guardium's VA solution for MongoDB Clusters can be run on mongos, a primary node and all secondary nodes for replica sets.
- Entitlement reports and Query Based Builder are not supported for MongoDB.

## MongoDB Datasource with SSL

You can import server cert which we do behind the scene for self signed. Customer can also import their certificate. Certificates also work on central manager and push down to collectors.

## CAS for MongoDB

The Mongo CAS Assessment template allows you to specify multiple paths in the datasource to scan various components of the file system.

## Teradata Aster

### Aster Data

Acquired by Teradata in 2011, typically used for data warehousing and analytic applications (OLAP). Aster Data created a framework called SQL-MapReduce that allows the Structured Query Language (SQL) to be used with Map Reduce. Most often associated with clickstream kinds of applications.

A security assessment should be created to execute all tests on the queen node. All database connections for Aster Data go through the queen node only.

Testing on worker and loader nodes is only required when performing CAS tests (File permission and File ownership).

Privilege tests loop through all the databases in a given Aster's instance.

## SAP HANA

SAP HANA is an in-memory, column-oriented, relational database management system developed and marketed by SAP SE. HANA's architecture is designed to handle both high transaction rates and complex query processing on the same platform.

- [\*\*Database privileges for vulnerability assessments and classification\*\*](#)  
Guardium provides a set of scripts to simplify the creation of groups or roles with minimum privileges required for running vulnerability assessments.
- [\*\*Deploying VA for Db2 for i\*\*](#)  
Enable a group of users to run vulnerability assessments, and configure and run the tests.
- [\*\*Using VA with Cloudera\*\*](#)  
Learn how to use Guardium vulnerability assessments with Cloudera distributions of Apache Hadoop.
- [\*\*Troubleshooting Cassandra\*\*](#)  
Troubleshooting DataStax Enterprise (DSE) Cassandra for Vulnerability Assessment (VA).

## Related concepts

- [License keys for Guardium Vulnerability Assessment](#)

## Database privileges for vulnerability assessments and classification

Guardium provides a set of scripts to simplify the creation of groups or roles with minimum privileges required for running vulnerability assessments.

## Before you begin

This task requires downloading scripts from a Guardium system and running those scripts on a database server. You will need to identify the IP address of the machine used to access the Guardium system. This could be the IP address of an individual workstation where you will download the scripts before transferring them to a database server, or it could be the IP address of the database server itself.

## About this task

A user requires access to the database and specific database privileges to run Guardium vulnerability assessments and Guardium classifier. Guardium provides a set of scripts to simplify the creation of groups or roles with minimum privileges required for running vulnerability assessments. Once created, these groups or roles can be assigned to any database user who needs to run an assessment. You will create a Guardium datasource with this user to perform the VA scan.

Scripts are provided to support most database types and are designed to be run in the database tool itself. Each script includes detailed instructions in the script header. The privileges granted for each database type can be seen in the script looking at each grants.

Important: Before running any scripts, database administrators should read the instructions in the script headers and review the database actions that will be taken by the script.

## Procedure

1. On a Guardium system, enable the file server using the **fileserver** CLI command.  
For example, to enable the file server for one hour and download the scripts to a system with IP address **10.0.0.1**, use the following command:

```
fileserver 10.0.0.1 3600
```

When successfully initiated, the file server should display output similar to the following:

```
Starting the file server...
The file server is ready at https://guardium.host.com:8445
The timeout has been set to 3600 seconds and it may timeout during the uploading.

The upload will only be accessible from the IP you are logged in from: 10.0.0.1

Press ENTER to stop the file server.
```

2. On the machine where you will download the scripts, use a web browser to access the file server.

For example, for a Guardium system running at <https://guardium.host.com:8445>, access the scripts for vulnerability assessment and classification at the following URLs:

[https://guardium.host.com:8445/log/debug-logs/gdmonitor\\_scripts/](https://guardium.host.com:8445/log/debug-logs/gdmonitor_scripts/)  
[https://guardium.host.com:8445/log/debug-logs/classification\\_role/](https://guardium.host.com:8445/log/debug-logs/classification_role/)

Important: Discovery processes of the Guardium classifier require a higher level of database access than is required for vulnerability assessment tests. It is recommended to use the scripts in `gdmonitor_scripts` for vulnerability assessment and the scripts in `classification_role` for the classifier.

3. Download the required scripts using the web browser's Right-click  $\rightarrow$  Save link as... action or a similar function.

Review the README.txt files to identify the correct scripts to use for specific database types.

Tip: The following scripts are for Microsoft SQL Server:

- `gdmonitor-mss.sql` is for Microsoft SQL Server
- `gdmonitor-mss-SA.sql` provides administrative privileges required for six of the Microsoft SQL Server vulnerability assessment tests. If you do not allow these privileges, the tests will return errors indicating inadequate privileges. These six tests represent no more than 5% of the available tests.

## What to do next

Once you have downloaded the scripts required for your database servers, closely review and follow the instructions in the script headers.

## Deploying VA for Db2 for i

Enable a group of users to run vulnerability assessments, and configure and run the tests.

### About this task

#### Deployment Steps

1. Vulnerability Assessment is deployed from the Guardium system.
2. User runs a Guardium-supplied script against the target database to create a role with the appropriate privileges. User then creates a datasource connection to the database.
3. Create a security assessment, then select your datasources and desired tests to execute.
4. Once the execution is done, a report is created, showing what tests have passed and/or failed along with detailed hardening recommendations.

IBM for i version support:

- IBM for i 6.1, 7.1 and 7.2 partitions
- VA test Coverage (115 tests in total)
- Profiles with Special Authorities
- Profiles with access to Database Function Usage
- Password policies
- Database Objects privilege granted to PUBLIC
- Database Objects privilege granted to individual user
- Database Objects privilege granted with grant option
- Security APARS
- Entitlement Reports
- Profiles with Special Authorities
- Group granted to user
- Database Objects privilege granted to PUBLIC
- Database Executable Objects privileges granted to PUBLIC
- Database Objects privilege granted to individual user
- Database Objects privilege granted with grant option

## Procedure

1. Use the Group Builder to create a group of users that you want to use VA. Open the Group Builder by clicking Setup  $\rightarrow$  Tools and View  $\rightarrow$  Group Builder. The next step uses a script for a group named `gdmonitor`.
2. Run the following script on your Db2 for i system to grant privileges needed for executing VA to the group. This is done outside the Guardium system using a database native client.

```
grant select on SYSIBADM.FUNCTION_INFO to gdmonitor;
grant select on SYSIBADM.FUNCTION_USAGE to gdmonitor;
grant select on SYSIBADM.GROUP_PROFILE_ENTRIES to gdmonitor;
grant select on SYSIBADM.SYSTEM_VALUE_INFO to gdmonitor;
grant select on SYSIBADM.USER_STORAGE to gdmonitor;
grant select on Qsys2.Authorizations to gdmonitor;
grant select on SYSIBADM.USER_INFO to gdmonitor;
grant select on QSYS2.SYSSCHEMAAUTH to gdmonitor;
grant select on QSYS2.SYSTABAUTH to gdmonitor;
grant select on QSYS2.SYSPACKAGEAUTH to gdmonitor;
grant select on QSYS2.SYSROUTINEAUTH to gdmonitor;
grant select on QSYS2.SYSSEQUENCEAUTH to gdmonitor;
grant select on QSYS2.SYSCOLAUTH to gdmonitor;
```

For IBM Db2 for i v7.1 and higher, also include the scripts:

```
grant select on QSYS2.SYSVARIABLEAUTH to gdmonitor;
grant select on QSYS2.SYSXSROBJECTAUTH to gdmonitor;
```

3. Create a JDBC connection to your Db2 for i system. To open the Select datasource window, browse to Setup > Tools and Views > Datasource Definitions. Click **+** to create a new datasource, and select Security Assessment as the application type. For more information, see [Creating a datasource definition](#).
- a. Click New and enter the appropriate information. For Connection Property, enter "property1=com.ibm.access.AS400JDBCDriver;translate binary=true".
4. Create an assessment using the Assessment Builder. Open the Assessment Builder by clicking Harden > Vulnerability Assessment > Assessment Builder.
- a. Enter a description for the assessment.
  - b. To add the datasource created in the previous step, click Add Datasource, select the datasource from the Select datasource, and then click Save. Note: You must click Apply to save the assessment before you can configure tests.
5. Add tests to the assessment by clicking Configure Tests. Click the IBM for i tab, select the tests that you want to add, and click Add Selections.
6. Click Return to go back to the Security Assessment Finder. Run the test by clicking Run Once Now, or schedule the test using Audit Process Builder. Open the Audit Process Builder by clicking Discover > Classifications > Audit Process Builder.
7. Click View Results to view the details of all the executed tests, including recommendations for improving your score.

## Results

What to do when a test fails?

- You can patch your database if it is relating to patches.
- You can re-configure database parameters to best practice recommendation.
- You can revoke objects or system privileges that are not required by your applications.
- You can revoke objects granted directly to grantee and grant the object privileges to a role/group and assign the grantee to that role/group.
- You can change password policy setting or change users default password.
- If your application required specific grant, you can create exception group and link that to your failed test and re-execute.

## Using VA with Cloudera

Learn how to use Guardium vulnerability assessments with Cloudera distributions of Apache Hadoop.

Cloudera Manager  
Datasource Setup

The Cloudera Manager datasource uses the Cloudera Manager Java API for a connection. It does not use JDBC.

The Cluster Name must be defined in the datasource GUI. The Cluster name is the Cluster display name in the Cloudera manager GUI on the left-hand side.



To execute Vulnerability Assessment tests for Cloudera Manager, you need to define a datasource user with the Read-Only role for most the Vulnerability Assessment tests. Then, there are a small number of Vulnerability Assessment tests which require the datasource user have the Cluster Administrator role as the minimum privilege to run the tests.

The following Vulnerability Assessment tests require the datasource user to have the Cluster Administrator role:

1. Authentication Backend Order
2. HTTP port for Admin Console
3. HTTPS port for Admin Console
4. Use TLS Authentication of Agents to server
5. Use TLS Encryption for Admin Console
6. Use TLS Encryption for Agents

This information is also available in the Cloudera Manager gdmmonitor script (`/log/debug-logs/gdmmonitor_scripts/gdmmonitor-Cloudera-Manager.sql`).

If SSL is enabled, check Use SSL and check Import server ssl certificate.

CAS Database Instance setting

The Account should be root.

The Directory will need to be defined as the Cloudera manager install path. For example: `installpath=/opt/cloudera`

Example of Cloudera Manager datasource settings.

**Update datasource**

---

|                                                                             |                                   |
|-----------------------------------------------------------------------------|-----------------------------------|
| * Application Type                                                          | Security Assessment               |
| * Name                                                                      | Cloudera Manager - PASS           |
| * Database Type                                                             | CLOUDERA MANAGER                  |
| Description                                                                 |                                   |
| <input type="checkbox"/> Share Datasource <a href="#">?</a>                 |                                   |
| <input checked="" type="checkbox"/> Use SSL <a href="#">Add Certificate</a> |                                   |
| <input checked="" type="checkbox"/> Import server ssl certificate           |                                   |
| Authentication                                                              |                                   |
| <input checked="" type="checkbox"/> Assign Credentials                      |                                   |
| * User Name                                                                 | gdmuser                           |
| * Password                                                                  | *****                             |
| Location                                                                    |                                   |
| * Host Name/IP                                                              | odh5mgr-va.guard.swg.usma.ibm.com |
| * Port number                                                               | 7184                              |
| * Cluster Name                                                              | cluster 2                         |
| Connection Property                                                         | Ex: prop1=value;prop2=value       |
| Custom URL                                                                  |                                   |
| <a href="#">Hide advanced options</a>                                       |                                   |
| <b>Roles</b> No roles have been assigned to this datasource.                |                                   |
| CAS Database Instance                                                       |                                   |
| Account                                                                     | root                              |
| Directory                                                                   | installpath=/opt/cloudera         |
| Severity Classification:                                                    | HIGH                              |
| Connection successful                                                       |                                   |

## Hive

### Datasource Setup

Use the Apache Hive JDBC driver 1.1.1.

Kerberos - The User Name and Password must be a valid Kerberos User ID and Password. It is also used for CA. Test to make sure your Kerberos User ID and Password can be used to login to the Hive beeline command line.

Make sure you have already created a Kerberos Configuration that defines your KDC and Realm for your appliance. On the Guardium GUI, go to Setup > Tools and Views > Kerberos Configuration. If no Kerberos Configuration has been created, then click on + icon to create a new Kerberos Configuration.

### Edit Kerberos Configuration

---

|                   |                                   |
|-------------------|-----------------------------------|
| * Name            | kerberos_hive                     |
| * KDC             | dbanetdc01.guard.swg.usma.ibm.com |
| * Realm           | DBANET.ROOT                       |
| * Encryption type | aes256-cts-hmac-sha1-96           |

---

**Save**

**Close**

After you have created a Kerberos Configuration, you can select it to configure your datasource setup.



If SSL is enabled, check "Use SSL" box and check the "Import server ssl certificate" box.

Note: Hive can only support either LDAP/SSL or Kerberos, not both.

#### CAS Database Instance setting

1. The Directory will need to be defined as the Cloudera manager install path. For example: installpath=/opt/cloudera
2. If HDFS is enabled for Kerberos, the Datasource User Name and Password must be a valid Kerberos User ID and Password. CAS scripts uses it for obtaining a Kerberos ticket.
3. The Account must be root. For certain parameter tests that require CAS, it is important that the CAS user is root in order to access the real-time configuration under the Cloudera agent process directory (/var/run/cloudera-scm-agent/process/).

Note: Guardium does not in any way modify or alter your configuration data.

For Hive

For the Privilege tests, the datasource account must be a member of the Sentry Admin group. See the Hive gdmonitor script for steps to check the Sentry Admin group.

When setting up Hive datasources, you can only perform a JDBC test connection when the datasource is pointing to your Hive server2. For all other Hive datasources, you can clone this specific datasource using nodename where the Cloudera service is installed. Make sure the cloned datasource has a valid Username and Password just like the Hive server2 datasource. For these datasources, you cannot perform a datasource test connection. However, Guardium relies on the accuracy of the Username and Password from the datasource to perform a Kerberos connection using CAS when Kerberos enabled.

Datasource Definition

Name: mms Hive cdh5ldap01-va\_kerberos

Database Type: HIVE

Severity classification: NONE

Description:

Share Datasource:

Use Kerberos:  Kerberos Config: kerberos\_hive

Realm: DBANET.ROOT

KDC: dbanetdc01.guard.swg.usma.ibm.com

Authentication

Save Password:

Login Name: vateam@DBANET.ROOT

Password: \*\*\*\*

Location

Host Name/IP: cdh5krb01-va.guard.swg.usma.ibm.com

Port: 10000

Service Name:

Informix Server:

Database:

Connection Property:

Custom Url:

CAS

Database Instance Account: root

Database Instance Directory: installpath=/opt/cloudera

Roles

No roles have been assigned to this datasource

Add Comments Test Connection Apply Back

#### Vulnerability Assessment Tests

The Hive Privilege tests require Sentry Services to be installed and configured. Without Sentry, there is no security. Everyone can connect to Hive and access data.

The Vulnerability Assessment CAS test for HDFS parameters are from configuration files under the Cloudera agent process directory (/var/run/cloudera-scm-agent/process/). The folder names inside these process directories change every time the Cloudera agent services are started.

Some of the HDFS parameter CAS tests require the datasource system to be a specific node configuration (for example, NameNode or DataNode). Some CAS tests require Yarn, Mapreduce or Hive Server to be installed on the datasource system. Please select the tests carefully for your assessment based upon your datasource system configuration. If the requirements are not met for the test, then the test will error with the recommendation to execute these tests on the correct Cloudera services. The requirements are also mentioned in the test description.

When creating a Hive datasource, it is recommended to have one datasource for each Cloudera service (NameNode, DataNode, HiveServer2, Hive metastore, Yarn NodeManager and Yarn ResourceManager).

Regardless of the number of nodes in your cluster, if you have Guardium Hive datasources that cover all of these services, you then have properly setup your environment to run Vulnerability Assessment.

For example

| dfs.namenode.name.dir Permissions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Not Applicable                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Test category: Com. Severity: Major                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | (1/9/17 3:17 AM) Current datasource environment is not setup as a Hadoop NameNode.             |
| This test is to ensure the "dfs.namenode.name.dir" directory permissions are set to "u=rwx,g=rx,o=rx". The "dfs.namenode.name.dir" HDFS property specifies where the name node should store the name table (fileimage) on the local file system. Securing HDFS files and directories will reduce the probability of unauthorized modifications to those resources. Namenode directories may contain sensitive information that should not be accessible by other accounts on the system. The value of this property may be a single directory or a comma-delimited list of directories. When it is a comma-delimited list of directories, each will contain the same information. This test only works on the Hadoop namenode. | Recommendation: This test is not valid for this datasource environment. No action is required. |
| Ext. Reference: Apache Hadoop in Secure Mode, Cloudera Security guide                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                |
| Cloudera Idap cdh5krb03.va                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                |
| Datasource type: HIVE Severity: None                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                |

## Troubleshooting Cassandra

Troubleshooting DataStax Enterprise (DSE) Cassandra for Vulnerability Assessment (VA).

### Troubleshooting data refresh issues

#### Issue

A new table or data is added or changed to the Cassandra database but is not reflected in the VA assessment results. You get an error in your test result or the datasource connection fails after the change is made.

Example: [DataDirect] [Cassandra JDBC Driver] [Cassandra]The server failed to respond to the connection request. Please verify the host and port specified. The non-thrift based Cassandra client port should be used, which on default Cassandra installs is 9042.

#### Possible cause

The local DataDirect Cassandra JDBC driver schema map file is corrupted or not up-to-date.

#### Description

To support SQL access to a noSQL Cassandra database, the DataDirect driver maps the Cassandra data model to a relational schema. The schema map files are saved in the location that is specified by the SchemaMap connection property. The driver looks for this file when it connects to the server. If the file does not exist, the driver creates one.

For Guardium, the SchemaMap is set to /var/log/guard/db\_driver/datastax/ <IP address>.config on the Guardium system.

#### Solution

1. In the Datasource Definition screen, set the Connection Property to CreateMap=forceNew.

When CreateMap is set to forceNew, the driver deletes the group of internal files that are specified by SchemaMap and creates a new group of these files at the same location. These internal files are required for a relational view of the native data, but they do not include schema map configuration file.

Guardium also runs the SQL extension refresh map when the CreateMap is set to forceNew. The refresh map statement adds newly discovered objects to your relational view of native data. It also incorporates configuration changes that are made to your relational view by reloading the schema map configuration file.

2. Test the connection to ensure that it is successful.

3. Remove the CreateMap=forceNew from your datasource connection property.

Note: This property forces the rebuild of internal files and involves the discovery of native data. If the size of your database is large, the schema maps can take time to build causing performance issues.

4. Save the datasource and run the assessment again.

### Troubleshooting consistency level issues

#### Issue

The error Cassandra code 4096 – Cannot achieve consistency level quorum appears in assessment report for some of the VA tests.

#### Possible causes

- Replication factors are not configured correctly for DSE security in production environments.
- Not all nodes in the cluster are up.

#### Solutions

##### Solution 1

1. Ensure that all nodes in the clusters are up and running.
2. Configure replication factors by changing the replication class to NetworkTopologyStrategy. Set the replication factor in the range 3 - 5 for the following security keyspaces. Do not set the replication factor greater than the number of nodes in the data center.
  - system\_auth
  - dse\_security
3. Run nodetool repair on the security keyspaces to repair the keyspace on all nodes to sync with each other. For more information, see the DSE administrator guide on the DataStax web page.
  - nodetool repair --full system\_auth
  - nodetool repair --full dse\_security
4. Run the assessment again.

##### Solution 2

1. In the Datasource Definition screen, set the Connection Property to ReadConsistency=one. When ReadConsistency is set to one, data is returned from the closest replica.

2. Save the datasource and run the assessment again.

## Set up your environment for Vulnerability Assessment

Set up your central manager and managed units for Vulnerability Assessment.

If you use Vulnerability Assessment (VA), it is recommended that your central manager is in the same data center as the managed units. Managed units that are running VA, access the central manager for definitions and content.

Note:

If a central manager is located in a different data center than the managed units, then environmental factors such as network latency, network congestion, and network traffic can impact performance when the centrally-managed definitions are retrieved.

For example, if your central manager and managed units are in different data centers, then you must set up your assessment and datasource definitions in your central manager, and run the assessment in the managed units. This set up might result in a significantly slower performance.

## Types of Vulnerability Assessments

Guardium® provides over two thousand predefined tests to check database configuration parameters, privileges, and other vulnerabilities. Some tests can also be customized to meet specific requirements.

### Vulnerability Assessment - Test types

A Vulnerability Assessment may contain one or more of the following types of tests: predefined or custom.

Predefined tests are designed to illustrate common vulnerability issues that may be encountered in database environments. However, due to the highly variable nature of database applications, some of these tests may be suitable for certain databases but totally inappropriate for others, even if they are within the same organization.

Guardium has enabled customization of some of the predefined tests to meet specific requirements of your organization. Additionally, to keep your assessments current with industry best practices and to protect against newly discovered vulnerabilities, Guardium distributes new assessment tests and updates on a quarterly basis as part of its Database Protection Subscription (DPS) Service. For more information, see [Installing IBM Security Guardium Database Protection Subscription \(DPS\) patches](#).

Predefined Tests include Privilege, Authentication, Configuration, Version, CVE, Security APAR, Query-based and CAS-based tests. Query-based and CAS-based tests may also be customized.

### Categories of Tests

The current categories with some high-level tests for security-related vulnerabilities include:

- Privilege
  - Object creation / usage rights
  - Privilege grants to DBA and individual users
  - System level rights
- Authentication
  - User account usage
  - Remote login usage
  - Password regulations
- Configuration
  - Database specific parameter settings
  - System level parameter settings
- Version
  - Database versions
  - Database patch levels
- Other
  - Installed sample databases
  - File ownership
  - File permissions

### CVE Tests

Guardium constantly monitors the Common Vulnerabilities and Exposures (CVE) from the MITRE Corporation and adds these tests for the relevant database related vulnerabilities.

### Security APAR Tests

Guardium adds predefined security Authorized Program Analysis Report (APAR) tests to monitor relevant database related vulnerabilities.

### Query-based Tests

A query-based test is either a predefined or custom test that can be quickly and easily created by defining your own test criteria. See [Defining a query-based test](#) for additional information on building a custom query-based test.

## CAS-based Tests

---

A CAS-based test is either a predefined or custom test that is based on a CAS template item of type OS Script command and uses CAS collected data.

Users can specify the template item and test it against the contents of the CAS results. See [Create a New Template Set](#) for assistance on creating an OS Script type CAS template.

Guardium is preconfigured with some CAS template items of type OS Script that can be used for creating a CAS-based test. These tests can be accessed through the CAS Template Set Definition panel and contain the word *Assessment*. For instance, the Unix/Oracle set for assessments is named Guardium Unix/Oracle Assessment. Additionally, any template added that involves file permissions will also be used for permission and ownership checking. See [Modify a Template Set](#) for viewing these template sets and seeing those items with type OS Script.

Both predefined and custom tests can be selected during the creation or modification of CAS-based tests. For more information, see [Defining a CAS-based test](#).

- [Defining a query-based test](#)

Create a test based on a query that runs an SQL statement.

- [Defining a CAS-based test](#)

Vulnerability Assessments use the CAS mechanism to run-OS level tests on the database server, and identify vulnerabilities.

---

## Defining a query-based test

Create a test based on a query that runs an SQL statement.

### About this task

---

You can create a new query-based test by using any of these approaches:

New

Start from the beginning and define all the fields.

Clone

Clone an existing query-based test.

Modify

Modify an existing query-based test.

## Procedure

---

1. Open the Assessment Builder by clicking Harden > Vulnerability Assessment > Assessment Builder.
2. From the User-defined tests, click Query-based Tests.
3. Click New, Clone or Modify to open the Query-based Test Builder.
4. Enter a unique Test Name.
5. Select a Database Type.
6. Select a Category.
7. Select a Severity.
8. Optional: Enter a Short Description for the test.
9. Optional: Enter an External Reference for the test.
10. Enter the Result text for pass that will be displayed when the test passes.
11. Enter the Result text for fail that will be displayed when the test fails.
12. Enter the SQL statement that will be run for the test.

Use the following convention to add and reference group members within a SQL statement:

For example:

To reference a group of users defined for the group MyUsersGroup and replace it with the actual members of the group use:

```
Select ... from DBA_GRANTS where ... AND USER in (~~G~MyUsersGroup~~) and ...
```

This will result in a SQL Statement such as the following where U1, U2, etc are the members of the MyUsersGroup group:

```
Select ... from DBA_GRANTS where ... AND USER in ('U1','U2','U3',...) and ...
```

If the group has no members, the database returns an error. In this case the reference is replaced with a single pair of quotation marks, like this:

```
Select ... from DBA_GRANTS where ... AND USER in ('') and ...
```

Use the following convention to replace a reference to a specific alias (of a specific group type) with the actual alias:

For example:

```
Select ... from USER_OBJECTS where ... AND OBJECT_TYPE = '~~A~GroupType~TYPE~~'
```

If there is an alias to TYPE of group type GroupType it will replace the string and the resulting SQL will look like:

```
Select ... from USER_OBJECTS where ... AND OBJECT_TYPE = 'TYPE'
```

where TYPE is the actual ALIAS

13. Optional: Enter a SQL Statement for Detail, a SQL statement that retrieves a list of strings to generate a detail string of Detail prefix + list of strings. See the example in Detail prefix.

Note: The detail generated is only displayed when the query-based test fails; allowing the user to enter a SQL statement that can retrieve the information that caused the test to fail and help identify the cause of failure.

- Note: Detail string can be seen within a Security Assessment Results by clicking on the Assessment Test Name and also queried through the Result Details attribute of the Test Result Entity.
14. Optional: Enter a Pre-test check SQL statement. This statement is run before running the test. If the statement returns 0, the test is not run. If the test returns 1 or an error, the test is run.
  15. Optional: Enter a Pre-test fail message. This message is inserted into the assessment results if the test is not run due to the SQL statement returning 0.
  16. Optional: In Loop databases, enter a list of databases through which the test should loop. The test returns the union or sum of the results returned from all the specified databases. You can use this function only when the test returns an integer value, and only with these database types: Informix, SQL Server, Sybase SE, PostgreSQL and MySQL. The looping is performed if the DB loop flag box is checked.  
One or more of the specified databases might be unavailable when the test is run. In that case the test will either skip that database and continue, or stop and issue a failure message, depending on whether the Skip on error box is checked.
  17. Optional: Enter a Detail prefix that will appear at the beginning of the detail string.

```
Example for SQL Statement for Detail & Detail prefix:
Test that checks for objects with certain grants.
Detail prefix: "Objects found with certain GRANT:"
SQL Statement for Detail: SELECT object FROM....--returning 4 records:
Obj1
Obj2
Obj3
Obj4
==> Details: Objects found with certain GRANT: Obj1, Obj2, Obj3, Obj4
```

18. Optional: Check the Bind output variable check box if the entered text in SQL statement is a procedural block of code that will return a value that should be bound to an internal Guardium® variable that will be used in the comparison to the Compare to value.

```
Example (Oracle):
declare
 retval integer := 0;
 strval varchar2(255) := '';
 nver number;
 sver varchar2(255) := '';
begin
 select VERSION
 into sver
 from V$INSTANCE;
 nver := to_number(substr(sver,1,(instr(sver,'.',1,2) - 1)));
 if nver >= 11.1 then
 select VALUE
 into strval
 from V$PARAMETER
 where NAME = 'sec_case_sensitive_logon';
 end if;
 if (nver < 11.1 or strval = 'TRUE') then
 retval := 0;
 else
 retval := 1;
 end if;
 ? := retval;
end;
```

19. Select the Return type that will be returned from the SQL statement.
20. Select the operator that will be used for the condition.
21. Enter in a Compare to value that will be used to compare against the return value from the SQL statement using the compare operator. It is this comparison that determines whether this test have passed or failed. You may also click on the RE (regex) to define a regular expression for the compare value.
22. Do one of the following:
  - Click Back to cancel changes and return to the previous screen.
  - Click Apply to save the query-based test.

## Results

---

You can add this newly created query-based test to an assessment.

## What to do next

---

### Defining a CAS-based test

Vulnerability Assessments use the CAS mechanism to run-OS level tests on the database server, and identify vulnerabilities.

### Before you begin

---

### About this task

---

You can create a new CAS-based test by modifying an existing CAS-based test or by starting from the beginning and defining all the fields.

### Procedure

---

1. Open the Assessment Builder by clicking Harden > Vulnerability Assessment > Assessment Builder.
2. From the User-defined tests, click CAS-based Tests to open the CAS-based Test Finder panel.
3. Click New or Modify to create a new test.
4. Enter a unique Test name.

5. Select a database from the Database Type menu.
6. Select a category from the Category menu.
7. Select a category from the Severity menu.
8. Optional: Enter a Short Description for the test.
9. Optional: Enter an External reference for the test.
10. Enter a Result text for pass that will be displayed when the test passes.
11. Enter a Result text for fail that will be displayed when the test fails.
12. Enter a Recommendation text for pass that will be displayed when the test passes.
13. Enter a Recommendation text for fail that will be displayed when the test fails. Recommendation text for fail - To prevent cross site hacking, any name from this list, used in the Recommendation text for fail text box, will be rewritten: expression; function; javascript; script; alert; eval; <img; ContentType
14. Select a template to use from the CAS Template menu.
15. Select an operator to use from the operator menu.
16. Enter a Search string that will be used with the operator to compare what is returned from the CAS template. This comparison that determines whether this test passes or fails. You may also click on the RE icon to define a regular expression for the search string.
17. Optional: Check the Fail if match check box if the test should fail when a match is made with the search string.
18. Click Apply to save the CAS-based test.

## Results

---

You can add this newly created CAS-based test to an assessment.

## Assessments

Assessments are a group of tests that scan database infrastructures for vulnerabilities and provide an evaluation of database and data security health with real-time and historical measurements.

- [\*\*Creating an assessment\*\*](#)  
Run security assessments against selected datasources to proactively identify and address vulnerabilities, improve configurations, and harden infrastructures.
- [\*\*Finding an assessment\*\*](#)  
Admins can find an existing vulnerability assessment by using the Security Assessment Finder screen.
- [\*\*Running an assessment\*\*](#)  
To get the results of an assessment, it must be run once it is created.
- [\*\*Viewing assessment results\*\*](#)  
You can take various actions while you view the results of an assessment.
- [\*\*Tuning a test\*\*](#)  
Tests can be optimized by adjusting parameters, applying group exceptions, and test detail exceptions.
- [\*\*Determining test severity\*\*](#)  
Considerations for determining and altering the severity of Vulnerability Assessment tests.
- [\*\*Deleting an assessment\*\*](#)  
You can delete an assessment and its dependencies.
- [\*\*Creating a test exception\*\*](#)  
When a test fails, you can apply an exception to the test. This exception allows the test to pass until a certain date, if specified, or indefinitely.
- [\*\*Group exceptions\*\*](#)  
Use a test exception to exclude specific members of a group from a security assessment. Run the security assessment against the exception group to see if a specific member of a group is affecting your assessment results. This is useful if you do not want to, or are not authorized to change group settings.
- [\*\*Test detail exceptions\*\*](#)  
A test exception can be fine-tuned by including an exception group, adding selected members to the exception group, and then adding test detail exceptions.
- [\*\*Adding custom comments to a test\*\*](#)  
Add custom comments to a vulnerability assessment test. These comments can be added to pre-defined or custom tests and can be exported or imported between Guardium systems.
- [\*\*Modifying the database version and patch level\*\*](#)  
Manually add the database version and patch level to override a failed vulnerability assessment.
- [\*\*VA summary\*\*](#)  
The following table list information per test and database key displayed in the VA summary table: test result by unique identifier; cumulative failed age; first failed date/ last failed date; last passed date; and, last scanned date. This information is tracked and users can create a report on this information.

## Creating an assessment

---

Run security assessments against selected datasources to proactively identify and address vulnerabilities, improve configurations, and harden infrastructures.

## About this task

---

The basic steps for creating a security assessment are:

1. Create the assessment
2. Add datasources to the assessment
3. Add tests to the assessment

## Procedure

---

1. Open the Assessment Builder by clicking Harden > Vulnerability Assessment > Assessment Builder.
2. To work with an existing assessment, click Clone or Edit to open the Security Assessment Builder window. Enter a new description, and modify only the fields that you want to change.

- If you are creating an entirely new assessment, complete all of the following steps.
3. In the Security Assessment Finder window, click New to create a new assessment.
  4. Enter a unique name for the assessment in Description.
  5. Optionally add an audit process that runs upon completion of the assessment.  
Note: Only audit processes with task types report or external feed can be assigned to a security assessment. You cannot run the audit process for a task that has the Remote Data Source parameter enabled.
  6. Click Add Datasource to open the Select datasource window. Select an existing datasource or click  to add a new datasource. For more information, see [Creating a datasource definition](#).
  7. To add a Datasource group, click Add Datasource Group.
  8. Add Roles to the Assessment, if applicable. You cannot assign roles to an assessment until you assign roles to the datasources it is based on.
  9. Click Apply to save the assessment.
  10. Add tests to the assessment by clicking Configure Tests.
    - a. From the Tests available for addition pane, select the appropriate tab for the datasource you added previously.
    - b. Select the tests that you want, and click Add Selections to add them to the assessment. Your selections appear in Assessment Test Selections.
    - c. Use the Assessment Test Selections to manage tests for your assessment. Delete any selected test, or click  to customize the test's parameters.
  11. Click Back to return to the Security Assessment Builder window. Click Return to return to the Security Assessment Finder.

## What to do next

---

From the Security Assessment Finder window, select the created assessment, and click Run Once Now to run your test.

---

## Finding an assessment

Admins can find an existing vulnerability assessment by using the Security Assessment Finder screen.

### Procedure

---

1. Access the Security Assessment Finder screen by clicking Harden > Vulnerability Assessment > Assessment Builder.
  2. Enter your search parameter in the search box.
  3. Click  to view the filtered assessments.
- 

## Running an assessment

To get the results of an assessment, it must be run once it is created.

Assessments can run in a serial or parallel mode. If more than one assessment is scheduled to run, the queue can be viewed through the Guardium Job Queue report. See [Viewing assessment results](#) for more information on the results of an assessment.

You can optionally define and schedule an automated process for running of an assessment definition. The Audit Process finder panel is the starting point for creating or modifying an audit process schedule. Create a schedule to automatically run your assessments by going to the Audit Process finder panel. See Compliance Workflow Automation for assistance in defining an audit process

## Multi-thread Assessment

---

Guardium can run multiple vulnerability assessments in parallel to optimize the performance and utilization of the CPU. The number of threads that can run in parallel can be identified by multiplying the number of CPU cores in the machine by 2.

As an example, if there are 4 CPU cores, then 8 would be the maximum number of processes that can be defined and run concurrently. The cap limit, irrespective of the number of CPU cores, is 100.

To retrieve or define the concurrency limit, see [Classification APIs](#).

---

## Viewing assessment results

You can take various actions while you view the results of an assessment.

### View Results of an Assessment

---

View the results of an assessment in the Query-Report Builder. Open the Query-Report Builder by clicking Investigate > Query-Report Builder, and use the filter to find the report you are looking for.

### Interpreting the Results of an Assessment

---

An assessment evaluates multiple tests based on multiple reports. The overall results are displayed in a separate browser window entitled Security Assessment Results and have the following sections:

## Assessment Identity

---

The Assessment results identifies:

- The assessment name
- The date and time the assessment was run
- The time period for the assessment
- The Client and Server IP addresses or subnets

## Assessment Selection

---

Use the drop-down menu to select and display past results for an assessment. The latest result is displayed by default.

## Assessment Results History

---

The Assessment Results History shows the percentage of tests passing over a period of time. Further recommendations to improve the percentage of passing tests are given under the Assessment Test Results section.

## View log

---

When clicked, the Execution Log will be displayed in a new window that shows the runtime execution of the assessment test. A timestamp, along with events, and messages can aid in the debugging of issues that might have caused certain tests to fail.

## Results Summary

---

A tabular graph summarizes all the tests that were executed within this assessment. The X-axis represents the test's severity (CRITICAL, MAJOR, MINOR, CAUTION, or INFO). The Y-axis represents the type of test (Privilege, Authentication, Configuration, Version, or Other). Within the grid is the representation of the number of tests that have either Passed, Failed, or had an Error when trying to execute. The tests that are not categorized as "Passed" or "Failed" are also listed as errors. As an example, if an error is displayed due to an unsupported database, you can see this detail when you filter on the error type. The number of tests represented in this grid are directly related to the detail for the assessment tests that is given under the Assessment Test Results section.

## Current filtering applied

---

If you would like to change the filtering from what is currently applied, use the following two options to filter the results as you would like:

Reset Filtering - Removes all filtering options selected through the Filter / Sort Controls options.

Filter / Sort Controls - Use this to open a filter/sort options for the report. Options allow you to filter by Severities, Datasource Severity Classification (DS sev. class), Scores (pass, fail, or error), and Test Types (Observed/Database type). The sort option allows you to sort across combinations of severity, score, and datasource. Click Apply when you would like the chosen filter/sort options to take effect.

## Assessment Test Results

---

The Assessment Test Results section provides a detailed description of the test taken, information about the target datasource and datasource severity classification, and the test's Pass/Fail status, severity, the external reference, and reason for the current status. Each test name is clickable and will filter all information off the report except for relevant information about that particular test. A hover-over feature on the Reason field will display the recommendation to help remedy failed or tests in error.

The assessment results include a count of the number of tests and the number of passed tests in each of these categories:

- CIS tests
- CVE tests
- STIG tests

These values are displayed in the assessment result viewer and available for reporting as part of the VA results domain.

## Datasource Details

---

When expanded, the Datasource Details section will show all of the datasources that were referenced within this assessment including the datasource's specific environmental information.

## CVE and CVSS information

---

CVE Records and CVSS information will be displayed in the Assessment test result viewer.

The reference links are clickable (opens new window). Either section will be absent when there is no corresponding record for a result.

The CVSS fields of interest are:

- CVSS Score
- Access Complexity
- Availability Impact
- Confidentiality Impact
- Integrity Impact
- Authentication
- Access Vendor
- Source

- Generated on Datetime

## Working with failed tests

---

If some of the tests in your assessment show a failed status, you might want to take one of these actions:

- Tune a test. For more information, see [Tuning a test](#).
- Create a test exception. For more information, see [Creating a test exception](#).
- Create an exception group. For more information, see [Group exceptions](#).
- Create a test detail exception. For more information, see [Test detail exceptions](#).

## Export to PDF or to SCAP or AXIS XML

---

You can generate a PDF version of Assessment result by clicking Download PDF.

Use the Download XML button to open two menu choices: Download as SCAP xml and Download as AXIS xml. Choose one of these selections in order to download to your workstation an XML file representing the displayed assessment results. The file can be formatted for Security Content Automation Protocol (SCAP) XML or Apache Extensible Interaction System (AXIS) XML, which is used by QRadar.

---

## Tuning a test

Tests can be optimized by adjusting parameters, applying group exceptions, and test detail exceptions.

### About this task

---

Use this procedure to add exceptions to a test by using the test tuning feature.

Note: Depending on the assessment, some tests are not designed to allow group exceptions and test detail exceptions.

### Procedure

---

1. Go to Harden > Vulnerability Assessment > Assessment Builder.
2. Select the assessment you want to edit, and click  . From the Security Assessment Builder screen, click Configure Tests to access the Assessment Test Selections.
3. From the tuning column, select the test you want to adjust and click  .
4. To customize your test's parameters, use the Tuning section.
5. Use the Exception Group section to add an exception group. Click on the Exception Group drop down box and select the exception group. You can optionally enter a start and end date for your selected exception, and include a justification.
6. Select Test Detail Exceptions to search for one or more assessments that use single or multiple datasources, or a group of datasources. For more information, see [List existing Test Detail Exceptions](#).
7. Click Save to save your adjustments.

### Related concepts

---

- [Determining test severity](#)

## Determining test severity

---

Considerations for determining and altering the severity of Vulnerability Assessment tests.

Guardium® Vulnerability Assessment is designed to help you to alter the severity for each vulnerability assessment (VA) test, including tests that are within different security assessments.

## Defining test severity

---

The Guardium Vulnerability Assessment research and development team determines the severity of specific benchmarks such as Security Technical Implementation Guides (STIG) or Center for Internet Security (CIS), by considering the following references along with Common Vulnerability Scoring System (CVSS) scoring for each specific Common Vulnerabilities and Exposures (CVE) test.

- Type of Vulnerability (CVEs)
- Configuration
- Privileges
- Authentication
- Database vendor's security guide (in collaboration with database vendor teams)
- Extensive industry research and expertise
- Compliance Benchmarks (STIGs and CIS)

A VA test can reference multiple benchmarks, vendors, and other security references in parallel.

## Determining the severity of CRITICAL and MAJOR tests

---

- Password default and password hardening policies are typically assigned with a CRITICAL severity as they are deemed to be important in making sure that database account authentication cannot be easily hacked.
- Default database ports can be vulnerable to a variety of security risks, including brute-force attacks, exposure of sensitive information, malware distribution, and DDoS attacks.
- Encryption protocols, encryption strengths, encryption at rest and various database defaults, which may have a negative impact to production databases.
- The highest concentration of configuration tests is in the severity: MAJOR, CRITICAL (highest in security impact), CAUTION, MINOR, and INFO. Severity is assigned based on the individual configuration and the database type.
- PUBLIC grants on objects are assigned the CRITICAL severity level based on CRITICAL system level roles, privileges, and authorities depending on the database types.
  - Most privilege tests are assigned with a CRITICAL or MAJOR severity. Some object types or privileges may be more sensitive than others and they are assigned with different severity levels (CRITICAL, MAJOR, MINOR, and CAUTION).

Guardium VA patch tests are recommendations to the DBA to patch their database server to the latest patch level when comparing to metadata derived from the quarterly DPS upload.

Beginning 2019 Q3 DPS (15 August 2019), changes to the CVE severity is made for new CVE tests. To be synced up based on CVE CVSS 3.0 scoring, each new CVE severity is defined based on the CVSS 3.0 score.

For more information on optimizing tests, see [Tuning a test](#).

## Deleting an assessment

You can delete an assessment and its dependencies.

You can delete a security assessment from the Security Assessment Finder UI or by running the GuardAPI command **grdapi delete\_assessment**. For more information, see [delete\\_assessment](#).

Note: When you force delete an assessment, all its dependencies are deleted even if the assessment has results or is used by an audit task. The assessment results are deleted when the system data is purged. For more information, see [store\\_purge\\_object](#).

## Creating a test exception

When a test fails, you can apply an exception to the test. This exception allows the test to pass until a certain date, if specified, or indefinitely.

### Procedure

1. In the Security Assessment Results screen, go the Assessment Test Results section.
2. Go to the Test/Datasource that failed and click on the Fail link. You can also click on the Add test exception link to pull up the same screen.
3. Select the Assessment scope. You can apply the exception to a specific security assessment, or to all assessments.
4. Select the Datasource scope. You can apply the exception to a single datasource, a datasource group, or all datasources. The Single datasource option applies to the current datasource.
5. The name of the Approver cannot be changed.
6. Add a Start date, End date, provide a Justification for the exception and click Save. If an end date is not specified, then the exception will never expire.
7. To add another exception, click on the View test exceptions link. This brings up a Confirmation screen that lists the existing test exceptions. You can create another test exception by clicking Create.

## Group exceptions

Use a test exception to exclude specific members of a group from a security assessment. Run the security assessment against the exception group to see if a specific member of a group is affecting your assessment results. This is useful if you do not want to, or are not authorized to change group settings.

### About this task

Use this procedure to add group exceptions to a test.

Note: Depending on the assessment, some tests are not designed to allow group exceptions and test detail exceptions.

### Procedure

1. Open the Group Builder by clicking **Setup > Tools and Views > Group Builder**.
  2. Select VA Tests Exception from the Group Type menu to view the list of predefined exception groups.
  3. Select a group from the Modify Existing Groups menu and click Modify.
  4. Add the group members that you want to exclude from the VA test.
  5. Open the Assessment Builder by clicking **Harden > Vulnerability Assessment > Assessment Builder**. Select an assessment from the Security Assessment Finder and click Configure Tests.
  6. Find the test you want add the exception to, and click the test's Adjust this test's tuning button from the Tuning column.
  7. Select your exception group from the menu, and click Save. Run your assessment again to see if the exception group affects the outcome of the test.
  8. You can also add a group exception when a test is tuned. For more information, see [Tuning a test](#).
- Note: By default, Guardium includes an exception group called IBM iSeries Profile User Exclusions. You can clone and modify this group to suit your needs. All the Database Objects privilege tests exclude default system schemas from Guardium groups.

## Test detail exceptions

A test exception can be fine-tuned by including an exception group, adding selected members to the exception group, and then adding test detail exceptions.

A test detail exception is highly customizable. It can be added to one test in one single assessment, or to all assessments. Within the assessment, it can be applied to one datasource only, or one group of datasources, or all datasources. You can also apply a start and end date, and provide a justification for the exception.

A test detail ID is generated for each test detail exception. This ID can be referenced by using guardAPI.

### Create a Test Detail Exception

To create a test detail exception, click the Create Test Detail Exception link from the Security Assessment Results screen.

1. Click  to create a new test detail exception.
2. Select the appropriate element type. Selecting Regular Expression returns all the test detail values that match with the string that is entered in Step 3. The matching values are highlighted with a green check mark in the test detail exception list. Expired exceptions are highlighted in red.
3. Enter the Regular Expression that can match a test detail.
4. Select the Assessment scope and Datasource scope, if applicable.
5. Enter the start and end date, if applicable. Provide a justification for the exception and click Save.

You can also edit an existing test detail exception, add it to a group, or create a new datasource group and merge it with an existing group.

Note: A test detail exception will exist indefinitely if an end date is not applied.

### List existing Test Detail Exceptions

Access the Test Detail Exceptions search from the Security Assessment Finder screen, the Assessment Test Selections screen, or the Assessment Test Tuning screen.

Use the following procedure to search for test detail exceptions.

1. In the Assessments drop down box, select one of the following options:
  - a. All assessments: This search option returns records that have a scope set to "All assessments".
  - b. Any assessment: This search option returns records where the scope is set to any single assessment. It also returns records that have the scope set to "all assessments".
  - c. To search for test detail exceptions in a single assessment, select the name of the assessment in which you want to run your search query.
2. Use the Datasource scope radio button to search for test detail exceptions within a Single datasource, Group of datasources, or extend your search to records that have the scope set to All datasources.
3. From the Datasource drop down box, select the name of your datasource. To extend the scope of your search across datasource groups, check the Included in datasource group check box.
4. Use the Datasource type drop down box to select the type of the datasource.
5. Select the relevant test from the Test drop down box.
6. Click Search to access the Test Detail Exceptions results. Use the results section to view the results, add, or modify exceptions.

## Adding custom comments to a test

Add custom comments to a vulnerability assessment test. These comments can be added to pre-defined or custom tests and can be exported or imported between Guardium systems.

### About this task

User-defined fields can be used to add custom descriptions to vulnerability assessment test results. As an example, add a custom risk score for your test to a user-defined field. Then, use the Query-Report builder to add the custom field to your custom report. You can then view the custom risk score when you generate the custom report.

When you export your vulnerability assessment test to another Guardium system, your custom comments are also exported.

The following procedure describes the method to add custom comments to a vulnerability assessment test by using the Guardium UI.

### Procedure

1. Browse to Harden > Vulnerability Assessment > Available Test Notes.
2. Select the Datasource type.
3. Select the Test name or Test ID.
4. Under the User-defined Comments section, add up to three custom references and comments to the selected test.
5. Click Save.

### What to do next

Add the user-defined fields to your custom report by using the Query-Report builder. Generate the report and view your custom description in the test results.

## Modifying the database version and patch level

Manually add the database version and patch level to override a failed vulnerability assessment.

## About this task

When the database version and patch level is lower than the defined levels, the security assessment is designed to fail. To override this, the recommended patch level and database version can be manually added to the Group Builder.

Note: For Netezza users, the database version and patch level must match the defined level for the security assessment to pass.

## Procedure

1. Open the Group Builder by navigating to Setup > Tools and Views > Group Builder.
2. Select your Database version+Patches.  
For example: Oracle Database Version+Patches.  
Tip: Filter the Group Builder by typing `patch` into the table filter.
3. Click  to modify.  
This opens the Edit Group window.
4. Open the Members tab and click  to add member.
  - a. Use the DB Ver. and Patches fields to enter the database version and patch level.
  - b. Click OK to add the group member.

Tip: Use an existing record to determine the syntax for DB Ver. and Patches fields.
5. Click Save.

## VA summary

The following table lists information per test and database key displayed in the VA summary table: test result by unique identifier; cumulative failed age; first failed date/last failed date; last passed date; and, last scanned date. This information is tracked and users can create a report on this information.

## VA Summary

The default summary key for ISO installations includes the datasource name, host, and port.

Use VA Summary Tracking in Query Builder to define queries and reports.

This table can be exported/imported. Import Data will override existing data on the Guardium system (per key).

Table 1. VA Summary

| Table Column        | Type        | Description                                                  |
|---------------------|-------------|--------------------------------------------------------------|
| VA_SUMMARY_ID       | Int         | Auto-increment – primary key                                 |
| DATA_SOURCE_HASH    | Varchar(40) | Hash for the Key                                             |
| DB_TYPE             | Varchar     | Database Type                                                |
| SERVICE_NAME        | Varchar     | Database instance Name (if part of the key, "N/A" otherwise) |
| DB_PORT             | Varchar     | Database Port (if part of the key, "N/A" otherwise)          |
| DB_HOST             | Varchar     | Host / IP (if part of the key, "N/A" otherwise)              |
| TEST_ID             | Int         | Id of the Test                                               |
| FIRST_EXECUTION     | DateTime    | First time the test was executed                             |
| LAST_EXECUTION      | DateTime    | Last time the test was executed                              |
| FIRST_FAIL          | DateTime    | First time the test failed on this DB                        |
| LAST_FAIL           | DateTime    | Last time the Test failed on this DB                         |
| FIRST_PASS          | DateTime    | First time the Test passed on this DB                        |
| LAST_PASS           | DateTime    | Last time the Test passed on this DB                         |
| CURRENT_SCORE       | varchar     | Pass / Fail / Error                                          |
| CURRENT_SCORE_SINCE | Datetime    | Date Since the test is in the current status                 |
| CUMULATIVE_FAIL_AGE | Int         | Cumulative fail age (in days)                                |
| CUMULATIVE_PASS_AGE | Int         | Cumulative pass age (in days)                                |

The CLI commands are: store va\_test\_show\_query and show va\_test\_show\_query. Use export va\_summary to export this information.

The GuardAPI commands to change or display the key are: grdapi modify\_va\_summary\_key and grdapi reset\_va\_summary\_by\_key. The GuardAPI command to reset cumulative ages, both pass and fail, is grdapi reset\_va\_summary\_by\_id. Use grdapi export\_va\_summary to export this information.

An additional parameter, datasourceName, has been added to grdapi reset\_va\_summary\_by\_key and grdapi modify\_va\_summary\_key.

The VA Summary entity has an additional attribute, Datasource Name, that is populated ONLY if the datasource name is part of the key.

Note: The GrdAPI command, modify\_va\_summary\_key, will allow the key to be empty by calling the GrdAPI with all four parameters: useHost, usePort, useServiceName, useDatasourceName, equal to false. In this case, when the key is empty, the VA Summary calculation is disabled (no summary data will be calculated, updated or saved).

## IBM Guardium Data Protection app in ServiceNow

You can configure IBM Security Guardium to track incidents, problems, and tasks discovered by Guardium using the external ticketing system ServiceNow®.

A certified ServiceNow application is available if you prefer to use ServiceNow as your response control center. The IBM Guardium Data Protection integration is available on the ServiceNow site and can "pull" data from IBM Guardium Vulnerability Assessment (VA) via REST-API. The app synchronizes VA test definitions, data-source definitions, database group definitions, and VA test result entries for tighter integration with ServiceNow modules such as: Configuration Management Database (CMDB), Vulnerability Response, and Configuration Compliance. You can start scanning jobs right from the ServiceNow user interface. Once the VA results are in ServiceNow, your ServiceNow assignment rules automatically assign tickets to the designated group.

If you do not want to use the ServiceNow app, VA also provides more traditional integration with ServiceNow using ServiceNow's Table API. This out-of-the-box integration can send failed vulnerability scan results from the Guardium to ServiceNow as Incidents. In addition, you can integrate ServiceNow into your Guardium system. For more information, see [Configuring an external ticketing system](#).

Note: This feature is available for Guardium® Data Protection 11.4 with bundle 11.0p441, 11.5 with bundle 11.0p525, and later releases.

For more information about the ServiceNow Guardium Data Protection app, see: <https://github.com/IBM/ServiceNow-Guardium-Vulnerability-Assessment#readme>

## Required schema change

The schema used by vulnerability assessment tests on IBM Db2® for z/OS® changed in Guardium V9.1. If you upgrade from a release prior to 9.1, you must update your database in order to continue using these tests.

## About this task

When you upgrade your Guardium® system to version 10.x, you must create new database tables on your database server. These tables add support for a new set of tests, but you must create them whether you want to use the new tests or not.

In prior releases you created and populated tables in the gdmonitor schema:

- GDMMONITOR.OS\_GROUP
- GDMMONITOR.OS\_USER

These tables are replaced by tables in the CKADBVA schema:

- CKADBVA.CKA\_OS\_GROUP
- CKADBVA.CKA\_OS\_USER

## Procedure

1. Install Guardium 10.x
2. Copy `create_CKADBVA-schema_tables_zOS.sql` from the `/var/log/guard/gdmonitor_scripts` directory on your Guardium system to your database server. Run the `fileserver` command on your database server to retrieve the file.
3. The script contains instructions that describe steps to be performed before and after running the script. Read these instructions and run the script.
4. Populate the new tables with data similar to the data that was stored in the old tables.

## Results

Your system is now configured to use current vulnerability assessment tests.

## What to do next

## Assessing RACF vulnerabilities

If you use IBM Db2® for z/OS®, you can use vulnerability assessment tests to assess your RACF vulnerabilities. You must have at least version 9.1 of Guardium installed to use RACF assessments.

## About this task

Assess your Resource Access Control Facility (RACF) privileges whether they are granted within the database or external to the database. The tests, that comprise the RACF vulnerability assessments, identify the access control for object privileges, database privileges, and system privileges.

In order to use these tests, you must obtain and install IBM Security zSecure Audit, Version 2.1. This product enables the commands that are used in these tests to interact with RACF.

Tests that examine entitlements do not return a pass/fail grade; they return a list of entitled users. Examples of these reports include table and view privileges granted to grantees and package privileges granted to grantees. In a large environment that includes very large numbers of users and applications, these reports generate an overwhelming amount of data. When you run these reports in such a large environment, the process can run for a long time and consume large amounts of resources, and it might eventually time out.

## Procedure

1. Upgrade the database schema used to support vulnerability assessment on your database server.
2. Install zSecure Audit on your database server.  
Use the instructions and tools that are provided with zSecure Audit to learn how to populate approximately 24 tables in the CKADBVA schema to support the new zSecure tests.
3. The zSecure team will issue a PTF that enables zSecure Audit to work with Guardium vulnerability assessment. Obtain this PTF and apply it according to the accompanying instructions.

## Results

---

Your system is now configured to take advantage of the new zSecure tests.

## What to do next

---

Choose the new tests that you want to run to assess your RACF vulnerabilities. Configure and run the tests.

## Configuration Auditing System (CAS)

---

The Configuration Auditing System (CAS) tracks and reports changes to the server environment; for example, modified configuration files, environment or registry variables, or other database or operating system components. Auditing includes executable files or scripts that are used by the database management system or the operating system. The data is available on the Guardium® system and can be used for reports and alerts.

Note: The Configuration Auditing System is supported only in English.

### CAS Agent

---

CAS is an agent that is installed on the database server and reports to the Guardium system whenever a monitored entity changes, either in content or in ownership or permissions. CAS shares configuration information with S-TAP, though each component runs independently of the other. After you install the CAS client on the host, configure the actual change auditing functions from the Guardium portal. For more information about installing CAS, see either [Prerequisites, installing, and running CAS on a Windows server](#) or [Prerequisites, installing and running CAS on a Linux, UNIX server](#), depending on your operating system.

### CAS Server

---

The CAS server is a component of Guardium and runs on the Guardium system. It runs as a stand-alone process, independent of the Tomcat application server. It is controlled through systemd.

The CAS server is configured to use only a few of the available processors on the Guardium system. The number of processors that CAS uses is determined by the *divide\_num\_of\_processors\_by* parameter, which is stored in the cas.server.config.properties file. The default value of *divide\_num\_of\_processors\_by* is 2. The number of available processors on the Guardium system is divided by this value. Therefore, even when CAS uses 100% of the CPU on the allocated processors, the remaining processors are available for use by other applications.

### Template Set

---

A CAS template set contains a list of item templates, bundled together, that share a common purpose such as monitoring a particular type of database (Oracle on UNIX, for example). Two types of CAS templates are available:

- Operating System Only (UNIX or Windows)
- Database (UNIX-Oracle, Windows-Oracle, UNIX-Db2, Windows-Db2, and so on.)

A database template set is always specific to both the database type and the operating system type.

### CAS Template Item

---

The definition or set of attributes of a monitoring task over a single Monitored Entity. Users can define new CAS tests by creating new CAS templates or users can use predefined CAS templates that can be modified.

A template item is a specific file or file pattern, an environment or registry variable, the output of an OS or SQL script, or the list of logged-in users. The state of any of these items is reflected by raw data, that is, the contents of a file or the value of a registry variable. CAS detects changes by checking the size of the raw data, or computing a checksum of the raw data. For files, CAS can also check for system level changes such as ownership, access permission, and path for a file.

In a federated environment where all units (collectors and aggregators) are managed by one manager, all templates are shared by both collectors and aggregators and you can use CAS data in reporting or vulnerability assessments. When the collector and aggregator (or host where archived data is restored) are not part of the same management cluster the templates are not shared. Therefore, you cannot use CAS data with vulnerability assessments (VA) even when the data is present. To use CAS with VA, export or import definitions to copy the templates from the collector to the aggregator (or restore target).

Note: It is recommended that you do not use CAS to monitor more than 10,000 files per client.

### Monitored Entity

---

The actual entity being monitored, can be A File (its content and properties), Value of an Environment Variable or Windows Registry, Output of an OS command or Script or SQL statement

### CAS Instance

---

Application of a CAS Template Set on a specific Host (creating an Instance of that Template Set and applying it on a specific host)

### CAS Configuration

---

A CAS configuration defines one or more CAS instances, each of which identifies a template set to be used to monitor a set of items on that host.

## Default Template Sets

---

For each operating system and database type supported, Guardium provides a preconfigured, default template sets for monitoring a variety of databases on either Unix or Windows platforms. A default template set is one used as a starting point for any new template set defined for that template-set type. A template-set type is either an operating system alone (Unix or Windows), or a database management system (DB2®, Informix®, Oracle, and so on.), which is always qualified by an operating system type - for example, UNIX-Oracle, or Windows-Oracle. Many of the preconfigured, default template sets are used within Guardium's Vulnerability Assessments where, for example, known parameters, file locations, and file permissions can be checked.

You cannot modify a Guardium default template set, but you can clone it and modify the cloned version. Each of the Guardium default template sets defines a set of items to be monitored. Make sure that you understand the function and use of each of the items monitored by that default template set and use the ones that are relevant to your environment. After defining a template set of your own, you can designate that template set as the default template set for that template-set type. After that, any new template sets defined for that operating system and database type are defined with your new default template set as a starting point. The Guardium default template set for that type is removed; it remains defined, but is not marked as the default.

## Rationale for creating template sets to meet specific database configurations

---

Although Guardium supplies predefined CAS template sets for each database type, the wide variety of possible database configurations means that you might need to tweak the predefined template sets or create new ones to meet all of your needs in a production environment -- particularly concerning database software and data file locations. Plan on creating additional templates if you want CAS to monitor ownership of, permissions on, and changes to your database files.

For example, the predefined CAS template set for Oracle contains these templates, among others:

- \$ORACLE\_HOME/oradata/../\*.dbf
- \$ORACLE\_HOME/oradata/../\*.ctl
- \$ORACLE\_HOME/oradata/../\*.log
- \$ORACLE\_HOME/../init\*.ora

As you can see, these file-pattern templates all start with the same root, \$ORACLE\_HOME (NOTE: This is not necessarily the \$ORACLE\_HOME environment variable that is defined on your database server. By preference, CAS uses the data source field *Database Instance Directory* as the value for \$ORACLE\_HOME).

It is possible that in a production environment your Oracle data files are not in the same directory tree, or even on the same device, as your log files. Furthermore, the Oracle configuration files might be in yet another location.

You might create additional CAS templates using absolute paths to allow CAS to find and monitor all of your Oracle files, for example:

- /u01/oradata/mydb/\*.dbf
- /u02/oradata/mydb/\*.dbf
- /u03/oradata/mydb/\*.dbf
- /u01/oradata/mydb/\*.ctl
- /u02/oradata/mydb/\*.ctl
- /u03/oradata/mydb/\*.ctl
- /home/oracle11/admin/mydb/bdump/\*.log
- /home/oracle11/product/11.1/db\_1/dbs/init\*.ora

You can even use additional environment variables that are defined in your Oracle instance account. As an example, if you have variables defined as \$ORA\_DATA1, \$ORA\_DATA2 and \$ORA\_SOFT you can use:

- \$ORA\_DATA1/mydb/\*.dbf
- \$ORA\_DATA2/mydb/\*.dbf
- \$ORA\_DATA1/mydb/\*.ctl
- \$ORA\_DATA2/mydb/\*.ctl
- \$ORA\_SOFT/admin/mydb/bdump/\*.log
- \$ORA\_SOFT/product/11.1/db\_1/dbs/init\*.ora

## Sourcing files from different locations

---

CAS templates assume that certain files, such as user profiles, are in specific locations. You can configure CAS to look for these files in other locations that you specify by using a regular expression. To use this feature, add the user\_profile\_files parameter to the cas.client.config.properties file in the config directory. The format for each entry is

*identifying\_string=comma-separated list of files*

For example, suppose that you want to find .profile files in any Db2 user's home directory. For this example we assume that the names of all of these home directories include the string "db2." Add this line to the properties file:

**user\_profile\_files=.\*db2.\*=.profile**

If you need to specify more than one pattern, use the bar symbol (|) to separate patterns. If you want to add the profiles of your mysql users to the previous entry, replace the previous example with this:

**user\_profile\_files=.\*db2.\*=.profile|.\*mysql.\*=.profile**

- [CAS server authentication with SSL](#)

You can provide different levels of CAS server authentication support, from a non-secure connection to a secure connection with a signed certificate.

- [Prerequisites, installing, and running CAS on a Windows server](#)

Learn about the Configuration Auditing System (CAS) prerequisites, and how to install the CAS agent on your database server.

- [Prerequisites, installing and running CAS on a Linux, UNIX server](#)

Learn about the Configuration Auditing System (CAS) prerequisites for Linux and UNIX servers, and how to install the CAS agent on your database server.

- [CAS start-up and failover](#)

Various failover and connect parameters can be modified through S-TAP Control Change Auditing.

- [CAS templates](#)

Guardium provides a set of CAS templates, one for each type of data repository.

- [Working with CAS templates](#)  
This section describes how to maintain CAS templates and template sets.
  - [CAS hosts](#)  
A Configuration Auditing System (CAS) host configuration defines one or more CAS instances.
  - [CAS reporting](#)  
This section describes Configuration Auditing System (CAS) reporting.
  - [CAS status](#)  
To open the Configuration Auditing System Status page, browse to Harden > Reports > CAS Status
- 

## CAS server authentication with SSL

You can provide different levels of CAS server authentication support, from a non-secure connection to a secure connection with a signed certificate.

In addition to the basic security SSL provides, Guardium® provides CAS Server authentication support on the CAS client that runs on the database server. Authentication guarantees that CAS client communicates only with Guardium's CAS server. Unauthenticated connections and Common Name (CN) mismatches are reported in the CAS log file.

After the CAS client is configured, when the CAS server starts it loads a signed certificate as well as a private key. The server assigns the certificate and the key to a server socket on which it accepts connections. You can choose to provide authentication from either the CAS client side or server side.

The CAS client supports authentication with the following connection modes. Depending on your requirements, set the following parameters in the guard\_tap.ini file.

Non-secure connection

Set use\_tls='0'.

Secure connection without authentication (without FIPS mode)

Set use\_tls='1' and guardium\_ca\_path=NULL.

These settings force CAS to use SSL to communicate with the CAS server (that is, CAS uses SSL without server authentication) and disables FIPS mode.

Secure connection with server authentication (FIPS mode)

Set use\_tls='1' and guardium\_ca\_path=<public key location>.

The CAS client uses the public key in a certificate to authenticate the CAS server.

To prepare the custom certificate,

1. Create a custom certificate by using the **create csr alias** CLI command and have it signed by a certificate authority (CA) such as Verisign as described in [Certificate CLI commands](#).

Note: When you create the certificate, enter cas as the response to Please enter a one-word alias to uniquely identify this certificate.

2. Add the custom certificate to tomcat keystore: After you have the signed certificate (or certificates), use the **store certificate keystore alias console** CLI command to store the certificates starting from the last certificate to the root certificate in the chain.

Note: Enter cas as the response to Please enter a one-word alias to uniquely identify this certificate.

3. Copy the certificate in PEM format (for example, ca.cert.pem) to the CAS client machine, in the <public key location> described in the guardium\_ca\_path parameter of the guard\_tap.ini file.

On the CAS client machine, you can either set guardium\_ca\_path in guard\_tap.ini to,

- The full path, including the actual public key file name.
- A directory name, where all of the public keys within this directory are used to authenticate the server.

If guardium\_ca\_path is set to a file or directory that doesn't contain the public key, the connection attempt fails.

The CAS server supports secure connection with server authentication and common name verification. The common name (CN) verification provides an additional check-in which the certificate CN from the server is compared with the certificate CN set in the sqguard\_cert\_cn parameter in guard\_tap.ini. If sqguard\_cert\_cn is NULL or empty, this check is disabled. Otherwise, the value of sqguard\_cert\_cn must be the same as the CN of the custom certificate stored in CAS server tomcat keystore.

## Related concepts

---

- [Certificate CLI commands](#)

## Prerequisites, installing, and running CAS on a Windows server

Learn about the Configuration Auditing System (CAS) prerequisites, and how to install the CAS agent on your database server.

## Prerequisites on Windows

---

Before you install CAS, make sure that Microsoft .NET 4.5 or later is installed. After .NET is installed, approximately 2 GB of disk space is required for CAS.

Note: If .NET is not already installed, Guardium automatically installs it. In this case, .NET requires an additional 5 GB of disk space.

To run in FIPS mode, the CAS client requires IBM Java 8 SR7 or later. For more information, see [Managing the TLS version](#).

Table 1. Port Requirements for Windows servers

| Port  | Protocol | Guardium® connection to ... |
|-------|----------|-----------------------------|
| 16017 | TCP      | Clear (open the port) CAS   |
| 16019 | TLS      | Encrypted CAS               |

## Installing CAS

---

Use one of the following methods to install CAS:

- From the Windows installer wizard. To install CAS directly from Windows, browse to the directory where you download the .zip file, extract the file contents, double-click Setup.exe and follow the instructions.
- From the command line interface, as described in [Installing CAS from the CLI](#).
- From the Guardium Installation Manager (GIM) as described in [Installing CAS with GIM](#).

## Reconfiguring JAVA\_HOME (JVM) location for CAS

---

In most cases, the installation program takes care of finding the JAVA\_HOME value. This value is placed in the CAS configuration file.

If for any reason (for example, you install a new Java™ version after the Guardium CAS product is installed), you need to change the location of JAVA\_HOME (JVM), use the following procedure.

- Locate and open the CAS configuration file for editing. The full path name of the configuration file is <installation directory>/cas/conf/casclient.cfg.
- Within the configuration file, locate the [RUNTIMELIB] section, and change the value of the JVM directory (JVM=C:\Java\jre\bin\classic\jvm.dll).
- Save the file and restart the CAS service (service name: casclient or display name: IBM Security Guardium Change Audit System).

- [Installing CAS from the CLI](#)

Use the command line interface (CLI) to create scripts that are useful for managing large Configuration Auditing System (CAS) deployments.

- [Installing CAS with GIM](#)

When you install the Configuration Auditing System (CAS) on your database servers with the Guardium Installation Manager (GIM) client, you can install, upgrade, and manage agents on individual servers or groups of servers. Available actions include monitoring processes that are installed under GIM control, modifying CAS parameters, and performing other management tasks.

## Related reference

---

- [Configuration Auditing System \(CAS\) parameters](#)
- 

## Installing CAS from the CLI

---

Use the command line interface (CLI) to create scripts that are useful for managing large Configuration Auditing System (CAS) deployments.

To install CAS from the command line, call **setup.exe** with the appropriate parameters, as follows:

**Setup.exe -PARAMETER value**

Note: Use a space between each parameter and value pair. Do not use an equal sign (=).

The following parameters are available:

Table 1. Parameters that require an input value.

| Parameter        | Description                                                                                   |
|------------------|-----------------------------------------------------------------------------------------------|
| -INSTALLPATH     | The installation directory. The default installation path is "C:\Program Files (x86)\IBM\CAS" |
| -APPLIANCE       | Required. Set the appliance address to which CAS connects.                                    |
| -LOCALIP         | Required. The IP address of the server where you are installing CAS.                          |
| -CUSTOMER        | Sets the customer name in the registry.                                                       |
| -COMPANY         | Sets the company name in registry.                                                            |
| -SERVICEUSER     | Specifies a user to run the service under.                                                    |
| -SERVICEPASSWORD | The password for the service user.                                                            |

Table 2. Parameters that do not require a value

| Parameter         | Description                                                                                                                                                                                 |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -INSTALLEDLOGPATH | Specifies the location for storing the CAS installer log files. Use this parameter if you want don't want to use the default location (C:\Program Files\IBM\Windows CAS).                   |
| -UNATTENDED       | Required. Install silently.                                                                                                                                                                 |
| -UNINSTALL        | Uninstall the CAS.                                                                                                                                                                          |
| -JVM              | Specifies the directory where jvm.dll can be found. If no value is provided, then the installer tries to find jvm.dll automatically. Check the installation log for file detection results. |

For example, to install CAS in unattended mode, create a command similar to the following command:

```
setup.exe -UNATTENDED -INSTALLPATH "C:\Program Files (x86)\IBM\CAS" -APPLIANCE 10.0.148.160 -LOCALIP 10.0.146.161
```

## Related concepts

---

- [Prerequisites, installing, and running CAS on a Windows server](#)
- 

## Installing CAS with GIM

---

When you install the Configuration Auditing System (CAS) on your database servers with the Guardium® Installation Manager (GIM) client, you can install, upgrade, and manage agents on individual servers or groups of servers. Available actions include monitoring processes that are installed under GIM control, modifying CAS parameters, and performing other management tasks.

## About this task

Verify the following before you begin:

- Review the Windows CAS installation requirements in [Prerequisites, installing, and running CAS on a Windows server](#).
- The database server and operating system are supported.
- The intended CAS installation directory is empty or does not exist.
- The GIM client is installed on the database server where you plan to install a CAS.
- The GIM client on the database server is communicating with the Guardium system.
- Obtain the CAS module from either [Fix Central](#) or your Guardium representative.

After you install a GIM client on the database server, installation of the CAS for Windows is scheduled from the Guardium system.

Note: You cannot modify the CAS\_INSTALL\_DIR parameter after the installation. All other parameters can be modified after installation.

## Procedure

1. Upload the Windows CAS module for installation.
  - a. On the Guardium system, browse to **Manage > Module Installation > Upload Modules**.
  - b. Click **Browse** and select the CAS module that you want to install.
  - c. Click **Upload** to upload the module to the Guardium system.  
After you upload the module, it is listed in the Import Uploaded Modules table.
  - d. In the Import Uploaded Modules table, click the check box next to the CAS module to install.  
The module is imported and made available for installation. After the module is imported, Guardium resets the Upload Modules page and clears the Import Uploaded Modules table.
2. Install the uploaded CAS modules:
  - a. Under **Choose Clients** select the GIM client where you want to install CAS and click **Next**.
  - b. On the **Choose Bundle** page, clear the **Show only bundles** checkbox and select the CAS build from the drop-down list. Then, click **Next**.
  - c. On the **Choose parameters** page, the CAS\_INSTALL\_DIR and CAS\_JVM\_PATH parameters display. Values for these parameters are required before you can proceed. The default CAS install directory is C:\Program Files (x86)\IBM\CAS. Supply these values and then click **Next**.
  - d. Confirm your installation parameters and client name and click **Install**. To install the CAS immediately, you can simply click **OK**.  
If you want to change the location of the CAS installer log files from the default (C:\Program Files\IBM\Windows CAS), use the parameter CAS\_INSTALLER\_LOG\_DIR.

## What to do next

In the Success window, click **Show Status** to open the Status window to monitor the software install or upgrade. Click  to refresh the results. If an installation or upgrade has a failed status, click **Uninstall** if the button is available. Otherwise, click **Reset connection**. You can also view the status of the module installation by reviewing the report at **Manage > Reports > Install Management > GIM Clients Status**.

To verify that the CAS is communicating with the Guardium system, browse to **Manage > Activity Monitoring > CAS Control** and reviewing the CAS status and configuration.

## Related concepts

- [Prerequisites, installing, and running CAS on a Windows server](#)

## Prerequisites, installing and running CAS on a Linux, UNIX server

Learn about the Configuration Auditing System (CAS) prerequisites for Linux® and UNIX servers, and how to install the CAS agent on your database server.

### Prerequisites for Linux or UNIX servers

- CAS works with the following Java™ distributions: IBM®, OpenJDK, or Sun.
- The CAS server must be a Guardium® collector. The CAS server parameter (CAS\_SQLGUARD\_IP to install CAS with GIM, or sqlguard\_ip if you install CAS from the command line) is required.
- To run in FIPS mode, the CAS client requires IBM Java 8 SR7 or later. For more information, see [Managing the TLS version](#).

Table 1. Disk Space Requirements for Linux or UNIX servers

| Disk Space                        | Description                                                                                                                                                                                                    |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CAS Program files, including Java | AIX® - 309 MB, HP-UX - 630 MB, Linux - 405 MB, Solaris - 390 MB<br>Java runtime environment (JRE) 1.8 or later is required for CAS. You must obtain and install a JRE yourself (due to licensing constraints). |

Table 2. Port Requirements for Linux, UNIX servers

| Port  | Protocol | Guardium connection to ... |
|-------|----------|----------------------------|
| 16017 | TCP      | Clear CAS                  |
| 16019 | TLS      | Encrypted CAS              |

## Installing CAS with GIM

You can install CAS as a bundle with the Guardium Installation Manager (GIM), in the same way you install any other module. Use the following process, which is described in detail in [Set up by client](#), to install CAS with GIM:

1. Browse to Manage...>Module Installation,>Set up by Client.
2. Select the server where you want to install CAS and then click Next.
3. Select the CAS bundle and click Next.
4. Enter the Java home parameter for CAS. For more information, see [Locating the Java home directory and version](#).
5. Click Install to install the CAS bundle.

Note: If your site installed CAS using GIM in v10.6 or earlier, and then you upgrade CAS using GIM, delete and then re-create the Template/Datasource mapping after you upgrade. For more information, see [CAS hosts](#).

## Installing CAS client from the command line

---

Take the following steps to install the CAS client from the CLI:

1. Log on to the database server system with the root account.
2. Run the **install** command:

```
<guard-cas-setup>.sh -- install --java-home <JAVA_HOME> [--install-path <INSTALL_PATH>]
{--stap-conf <FULL_PATH_TO_GUARD_TAP_INI> | --sqlguard_ip <IP_OF_GUARDIUM_COLLECTOR>}
```

Where:

- <guard-cas-setup> - Identifies the name of the script file.
- -- install - Indicates an installation of CAS.
- --java-home - Identifies the JAVA\_HOME directory.
- --install-path - Identifies the installation path. You can specify the directory where you want to install the CAS client. Create the directory from root (make sure that the permissions are set to 755). If you do not include a directory in the installation path, Guardium automatically creates the directory for you.  
Note: If you install CAS on an AIX server, make sure that enough space is available to process the data segments (as defined in the data parameter of the AIX /etc/security/limits file). The default, and recommended value, for the data parameter is -1 (*unlimited*). However, if your site requires an actual value, Guardium suggests that you set this limit to at least 1 GB.  
If you modify /etc/security/limits, you might need to restart your server.
- You must include one of the following parameters:
  - --stap-conf - Use when the guard\_tap.ini file is located in the specified **stap-conf** directory. The installer uses the guard\_tap.ini file as-is.
  - --sqlguard\_ip - Use the default .ini file provided by the installer. In this case, the installer modifies the sqlguard\_ip key inside the .ini file with the value that is provided by the **--sqlguard\_ip** parameter.

Note: You must specify either **--stap-conf** or **--sqlguard\_ip**.

Note: For more information about modifying the guard\_tap.ini file, see [Editing the S-TAP configuration parameters](#)

## Uninstall a CAS client

---

Enter the following command to uninstall a CAS client.

Note: To ensure that the CAS client is completely uninstalled, call **uninstall** from a directory that is above the <INSTALL\_PATH>. The CAS files are not removed if you run the command from the <INSTALL\_PATH> or any directory underneath it.

```
<INSTALL_PATH>/bin/guard-cas-setup uninstall
```

## Start and stop CAS from the command line

---

Depending on your install or uninstall scenario, you might need to start and stop CAS from the command line.

To start or stop CAS, log on to the database server system with the root account. Depending on your operating system, use one of the following methods.

- For Red Hat® Enterprise Linux 6: Stop or start CAS with the **stop cas** or **start cas** commands.
- For Red Hat Enterprise Linux 7: Stop or start CAS with the **systemctl stop guard\_cas** or **systemctl start guard\_cas** commands.
- For other operating systems:
  1. Comment out (to stop CAS) or undo the comment (to start CAS) for the CAS agent entry in the /etc/inittab file. By default, the statement is as follows:

```
cas:<nnnn>::respawn:/usr/local/guardium/guard_stap/cas/bin/run_wrapper.sh /usr/local/guardium/guard_stap/cas/bin
```

2. Save the /etc/inittab file.
3. Run the **init q** command

- To validate whether CAS is running, enter the **ps -fe | grep cas** command.
- [Locating the Java home directory and version](#)

Locate the home directory and check the Java version before you install CAS.

## Related reference

---

- [Configuration Auditing System \(CAS\) parameters](#)

## Locating the Java home directory and version

---

Locate the home directory and check the Java™ version before you install CAS.

## About this task

---

When you install CAS on a UNIX system, you need the following information about Java on your system:

- Identify the JAVA\_HOME directory. You are prompted for its location during the CAS installation.
  - Verify that a supported version of Java is installed. If a supported version is not installed, you must install it before you install CAS.
- Note: To use CAS over SSL in a FIPS-compliant environment, you must install IBM® Java on the server where the CAS agent runs.

The **java** command contains the JAVA\_HOME directory. For example, if the JAVA\_HOME directory is:

```
/usr/local/j2sdk1.4.2_03
```

Then, the **java** command is:

```
/usr/local/j2sdk1.4.2_03/bin/java
```

## Procedure

---

1. To determine your location and version of Java, use the **which java** command. For example,

```
[root@yourserver ~]# which java
/usr/local/j2sdk1.4.2_03/bin/java
```

The JAVA\_HOME directory is `/usr/local/j2sdk1.4.2_03`.

2. If the **which java** command returns a symbolic link, use the **ls -ld <symbolic\_link>** command to determine the real Java directory name.
3. If the **which java** command returns the message `command not found`, then Java might be installed, but is not included in the PATH variable. In this case, use the **find** command to locate the Java directory; for example,

```
[root@yourserver ~]# find . -name java
./usr/bin/
```

4. To check the version number, from the java directory, run the **java -version** command. For example,

```
[root@yourserver ~]# /usr/local/j2sdk1.4.2_03/bin/java -version
java version "1.4.2_03"
Java(TM) 2 Runtime Environment, Standard Edition (build 1.4.2_03-b02)
Java HotSpot(TM) Client VM (build 1.4.2_03-b02, mixed mode)
```

5. Note the Java version that is returned. You are not prompted for this information, but if an issue arises later, you can eliminate the possibility of an unsupported Java version.

---

## CAS start-up and failover

Various failover and connect parameters can be modified through S-TAP Control Change Auditing.

When the CAS client starts on the host, it looks for a checkpoint file that it may have written to the system. This file tells CAS what it was doing the last time it was running. CAS then connects to its Guardium® system. If it has found a checkpoint file, CAS will ask the Guardium system to verify its version of its monitoring assignment against what is stored in the Guardium database. While the CAS client and the Guardium system have been disconnected, there may have been changes to the assignment. When any differences are resolved, CAS will resume monitoring. If CAS does not find a checkpoint file, it will ask the Guardium system what it should do. If the Guardium system finds the CAS host in its database, then the associated template sets will be sent to the CAS client, expanded into monitored items, and monitoring will begin. If the Guardium system cannot find the CAS host in its database, it will add it to the database and send the default template set for the CAS host operating system.

When connectivity is lost between the CAS client and Guardium system, it may take the CAS client and Guardium system up to five minutes (the wait time for a CAS client to expect a message from the Guardium system) to discover that it has lost contact with the primary Guardium system, but may happen sooner if the communication error is detected.

If the CAS client loses its connection to the Guardium system or cannot make an initial connection, it opens a failover file and begins writing the messages that it would have sent to the Guardium system, to the failover file. The path to this fail over file is stored in `guard_tap.ini` with the name `cas_fail_over_file`. When communication is reestablished the CAS client shuts down and restarts, sends all messages stored in the failover file to the Guardium system, and deletes the file. If the CAS client was unable to make the initial connection, it will use the checkpoint file to determine what to monitor, and continues doing what it was doing before communication failed.

When communication is lost, the client also starts a thread which periodically tries to reconnect with the primary Guardium system. The number of times CAS will attempt to reconnect, and the average time interval between reconnect attempts, are configurable parameters. It will try to reconnect for a period of time set in `guard_tap.ini` with the name `cas_server_failover_delay`. After that time has passed, the client will also try to connect to any secondary servers identified in `guard_tap.ini`. The secondaries will be tried in the order of the value of the `primary` attribute listed in the `SQL_Guard` sections of `guard_tap.ini`. When `primary` is not 1, it is a secondary. While the client is connected to a secondary server it will continue to try to reconnect to the primary server.

If the reconnect attempt limit is met, the CAS client stops trying to reconnect, but continues to write data to a failover file. To cap disk space requirements on the database server, there are actually two failover files. CAS writes to one file until it reaches its maximum failover file size (which is configurable), and then switches to the other, overwriting any previous data on that file. The default failover file size is 50MB (for each of the files).

You can specify one or more secondary Guardium systems when configuring the CAS client. In failover mode, CAS only tries to reconnect to its primary server until the time specified by `cas_server_failover_delay` in `guard_tap.ini` is exceeded. At that time, CAS begins trying to connect to any of the secondary servers, as well as its primary server (which is always the first server it tries to connect with during any reconnect attempt). While it is connected to a secondary server, CAS continues to try to reconnect to its primary server.

Changes to the CAS client configuration can only be made from the primary server and only while the host is online. Whenever the configuration of the CAS client is changed on the primary server and Guardium system is in standalone configuration, an export file is saved on the host. If the CAS client connects to a secondary server, the saved export file is imported from the host to the secondary server.

There is no need to separately maintain configurations on both primary and secondary servers. However, if on the primary server, the parameters for an individual monitored item have been changed from those defined in the template, then these changes will not be transferred to the secondary server. For example, even if the test interval on a particular file was changed from the template default of 1 hr to 10 min, the test interval on the secondary server will again be 1 hr. Essentially, monitored items are regenerated from the templates of the imported configuration. The delay before searching for secondary servers is based directly on time rather than failover file size. The delay is set with the `cas_server_failover_delay` parameter in `guard_tap.ini` and has a default of 60 minutes.

Various failover and connect parameters can be modified through S-TAP Control Change Auditing.

As with S-TAP, CAS connectivity outages create exceptions on the Guardium system, so alerts can be issued within moments of detecting the outage.

## Setting Up and Maintaining Secondary Servers

In the S-TAP/CAS configuration file on the database server system, one or more secondary Guardium servers can be defined. If the primary Guardium server becomes unavailable, CAS on that database server system will connect to a secondary Guardium system (as described previously, see Start Up and Failover).

### Rules of Failover

| Rule # | Guardium system | Fails over to               | Valid |
|--------|-----------------|-----------------------------|-------|
| 1      | stand alone     | stand alone                 | Yes   |
| 2      | managed         | managed (same manager)      | Yes   |
| 3      | managed         | managed (different manager) | No    |
| 4      | managed         | stand alone                 | No    |
| 5      | stand alone     | managed                     | No    |

### CAS Failover Limitations

1. CAS instances will not be relocated to the failed-over Guardium system when the source Guardium system is a managed unit and the target Guardium system is either:
  - a stand-alone Guardium system
  - a managed unit which is being managed by a different manager
2. CAS import/export option will be limited to manager and stand-alone machines only.

### Exporting CAS Hosts

1. Click **Manage > Aggregation & Archive > Export** to open the Definitions Export panel. Select CAS Hosts from the Type menu, select the to-be exported definitions from the Definitions to Export menu, and click .in the Export
2. A file named `exp_<date>_<time>.sql` is saved on your system. This file will contain the definitions of all CAS hosts selected, and the definitions of any template sets used by those CAS hosts.

### Importing CAS Hosts

1. Click **Manage > Aggregation & Archive > Import** to open the Definitions Import panel.
2. Use the Browse and Upload buttons to select files and upload them, then select the definition from the Import Uploaded Definitions pane.
3. Click **Import this set of definitions**  to import the definition.
4. Confirm the selected action (or not).  
Note: An import operation does not overwrite an existing definition. If you attempt to import a definition with the same name as an existing definition, you are notified that the item was not replaced. If you want to overwrite an existing definition with an imported one, you must delete the existing definition before performing the import operation.

### Maintaining Secondary Servers for a CAS Host

CAS configurations can also be maintained through the use of export and import operations. Since the import operation will not replace an existing definition, on each secondary server you must delete the old CAS host definition before importing the new one.

Be sure to perform this procedure only while the selected CAS host is connected to its primary server.

1. Export the definition of the CAS host (see the previous section).
2. On each secondary server:
  - Delete the old CAS host definition that you want to replace.
  - Import the definitions that were exported from the primary server (see Importing CAS Hosts, previous).

### CAS Client Ignore Change Alerts

The CAS client agent can avoid sending change notifications to the CAS server based on a predefined settings.

The CAS client agent will now look for a new parameter `ignore_change_alerts` in the CAS client agent's `cas.client.config.properties` configuration file.

If the parameter is not found or not set, the CAS client will work without any changes and the Ignore change alerts functionality will not be enabled (for example, the CAS client will alert on any file change).

If the new parameter is set, CAS client agent will ignore sending change notifications based on the change-types specified in the parameter value.

The possible change-types are:

`PERMISSION, SIZE, OWNER, GROUP, TIMESTAMP`

Ignoring multiple change-types can be set by + delimited concatenation of any of the specified change-type.

For example:

In order to avoid sending change notification on OWNER and GROUP changes, set up the parameter as follows:

`ignore_change_alerts=OWNER+GROUP`

Note: In the initial installation or when defining a new template, the FIRST scan of the files will be performed and these files will appear in the CAS changes report regardless to settings of Ignore change alerts.

## Correcting an invalid non-IP hostname

---

In case the user installs CAS agent with a bogus tap\_ip, guard\_tap.ini param, or CAS\_TAP\_IP (GIM param), Windows datasources defined for that host might be useless (if used for activity that requires accessing the remote database).

If the scenario happens, the user will have to delete the datasource and change the tap\_ip parameter to the correct database server hostname/ip.

---

## CAS templates

Guardium provides a set of CAS templates, one for each type of data repository.

### CAS templates - Db2

---

#### OS Script

Designates an OS script to run. Must begin with the variable \$SCRIPTS, which refers to the scripts directory beneath the CAS home directory, and identify the script to run, e.g., \$HOME/ db2\_spm\_log\_path\_group\_test.sh". The script itself must, of course, reside in the CAS \$SCRIPTS directory. Output from the script is stored in the Guardium® database to be used by security assessments. This can be either a shell or batch script to run, or a set of commands to enter on the command line. Because of the fickle nature of Java's parsing, it is suggested that you put all but the simplest commands into a script rather than run directly. On UNIX the script is run in the environment of the OS user entered. Three environment variables will be defined for the run environment which the user could use in writing scripts: \$UCAS is the DB username, \$PCAS is the DB password, and \$ICAS is the DB instance name. For Windows these three values will be appended as the last three arguments to the batch file execution. For example, if you had an OS Script template %SCRIPTS%\MyScript.bat my-arg1 my-arg2, then %3, %4 and %5 would be the DB username, password, and instance name respectively.

#### File

Designates a file to be tracked and monitored by security assessments. The path to the file can be absolute, or relative to the \$INSTHOME variable. Set the value of the \$INSTHOME variable in Database Instance Directory on the Datasource Definition panel. This is assumed to name a single file. Environment variables from the OS user environment can be used in the file name and will be expanded. For example, \$HOME/START.sh will name the startup script in the DB2® user's home directory.

#### File Pattern

Designates a group of files to be tracked and monitored by security assessments. The path to the files can be absolute, or relative to the \$INSTHOME variable. Set the value of the \$INSTHOME variable in Database Instance Directory on the Datasource Definition panel. A.. in the path indicates one or more directories between the portion of the path before it and the portion of the path after it. A.+ in the path indicates exactly one directory between the portion of the path before it and the portion of the path after it. For example: \$INSTHOME/sql11ib/../\* is just a short-hand for creating many single file identifications from a single identification string, a file pattern which will match all files in the directory. A file pattern can be viewed as a series of regular expressions separated by '/'. A file is matched if each element of its full path can be matched by one of the regular expressions in order. If an element of the pattern is an environment variable, it is expanded before the match begins. If .. is one of the elements of the pattern, it will match zero or more directory levels. For example, /usr/local/..foo will match /usr/local/foo and /usr/local/gunk/junk/bunk/foo. Using more than one .. element in a file pattern should not be necessary and is discouraged because it makes the pattern very slow to expand. Because of the confusion with its use in regular expressions | cannot be used as a separator as it might be in Windows.

Additionally, the Guardium UNIX/Db2 Assessment: UNIX - Db2 for UNIX set includes the following templates:

#### Db2govd Setuid Bits Is Not Set

This test monitors that the SETUID bit on Db2GOVD has been disabled

#### Db2start Setuid Bits Is Not Set

This test monitors that the SETUID bit on Db2START has been disabled

#### Db2stop Setuid Bits Is Not Set

This test monitors that the SETUID bit on Db2STOP has been disabled

#### File ownership

This test monitors file ownership, and changes thereto, of Db2 files.

#### File permissions

This test monitors file permissions, and changes thereto, of Db2 files.

### CAS templates - Informix

---

#### OS Script

Designates an OS script to run. Must begin with the variable \$SCRIPTS, which refers to the scripts directory beneath the CAS home directory, and identify the script to run, e.g., \$HOME/ informix\_rootpath\_owner.sh". The script itself must, of course, reside in the CAS \$SCRIPTS directory. Output from the script is stored in the Guardium database to be used by security assessments. This can be either a shell/batch script to be run, or a set of commands that could be entered on the command line. Because of the fickle nature of Java's parsing it is suggested that any but the simplest commands be put into a script rather than run directly. On UNIX the script is run in the environment of the OS user entered. Three environment variables will be defined for the run environment which the user could use in writing scripts: \$UCAS is the DB username, \$PCAS is the DB password, and \$ICAS is the DB instance name. For Windows these three values will be appended as the last three arguments to the batch file execution. For example, if you had an OS Script template %SCRIPTS%\MyScript.bat my-arg1 my-arg2, then %3, %4 and %5 would be the DB username, password, and instance name respectively.

## File

Designates a file to be tracked and monitored by security assessments. The path to the file can be absolute, or relative to the \$INFORMIXDIR variable. Set the value of the \$INFORMIXDIR variable in Database Instance Directory on the Datasource Definition panel. This is assumed to name a single file. Environment variables from the OS user environment can be used in the file name and will be expanded. For example, \$HOME/START.sh will name the startup script in the Informix® user's home directory.

Additionally, the Guardium UNIX/Informix Assessment for UNIX set includes the following templates:

Scan log files for errors

This test monitors for error in the online.log file

File ownership

This test monitors file ownership, and changes thereto, of Informix files.

File permissions

This test monitors file permissions, and changes thereto, of Informix files.

## CAS templates - Oracle

---

### OS Script

Designates an OS script to run. Must begin with the variable \$SCRIPTS, which refers to the scripts directory beneath the CAS home directory, and identify the script to run, e.g., \$SCRIPTS/oracle\_user.sh. The script itself must, of course, reside in the CAS \$SCRIPTS directory. Output from the script is stored in the Guardium database to be used by security assessments. (This can be either a shell/batch script to be run, or a set of commands that could be entered on the command line. Because of the fickle nature of Java's parsing it is suggested that any but the simplest commands be put into a script rather than run directly. On UNIX the script is run in the environment of the OS user entered. Three environment variables will be defined for the run environment which the user could use in writing scripts: \$UCAS is the DB username, \$PCAS is the DB password, and \$ICAS is the DB instance name. For Windows these three values will be appended as the last three arguments to the batch file execution. For example, if you had an OS Script template \$SCRIPTS/mysql\_mysqld\_user.sh, then %3, %4 and %5 would be the DB username, password, and instance name respectively.)

### File

Designates a file to be tracked and monitored. The path to the file can be absolute, or relative to the \$ORACLE\_HOME variable. The value of the \$ORACLE\_HOME variable is the value you set in the Database Instance Directory field of the Datasource Definition panel. (This is assumed to name a single file. Environment variables from the OS user environment can be used in the file name and will be expanded. For example, \$HOME/START.sh will name the startup script in the Oracle user's home directory.)

### File Pattern

Designates a group of files to be tracked and monitored. The path to the files can be absolute, or relative to the \$ORACLE\_HOME variable. Set the value of the \$ORACLE\_HOME variable in Database Instance Directory on the Datasource Definition panel. A .. in the path indicates one or more directories between the portion of the path before it and the portion of the path after it. A .+ in the path indicates exactly one directory between the portion of the path before it and the portion of the path after it. For example: \$ORACLE\_HOME/oradata/../\*.dbf (This is just a short-hand for creating many single file identifications from a single identification string, a file pattern. A file pattern can be viewed as a series of regular expressions separated by /'s. A file is matched if each element of its full path can be matched by one of the regular expressions in order. If an element of the pattern is an environment variable, it is expanded before the match begins. If .. is one of the elements of the pattern, it will match zero or more directory levels. For example, /usr/local/..foo will match /usr/local/foo and /usr/local/gunk/junk/bunk/foo. Using more than one .. element in a file pattern should not be necessary and is discouraged because it makes the pattern very slow to expand. Because of the confusion with its use in regular expressions | cannot be used as a separator as it might be in Windows. The file pattern shown previously is not correct because \*.dbf is not a valid regular expression. It should be \*.dbf.

Additionally, the default Guardium UNIX/Oracle template set includes the following templates:

### ADMIN\_RESTRICTIONS Is On

This test monitors that the listener.ora parameter ADMIN\_RESTRICTIONS is set properly.

### File ownership

This test monitors file ownership, and changes thereto, of the Oracle data files, logs, executables, etc.

### File permissions

This test monitors file permissions, and changes thereto, on the Oracle data files, logs, executables, etc.

### Scan log files for errors

This test scans the Oracle log files for occurrences of error strings.

### SPOOLMAIN.LOG Does Not Exist

This test checks the existence of the Oracle SPOOLMAIN.LOG.

## CAS templates - MongoDB

---

MongoDB is typically used as an operational system and as a backend for web applications due to ease of programming for non-relational formatted data like JSON documents.

Use the UNIX/MongoDB template to specify multiple paths and multiple directories in the datasource to scan various components as specified in the MongoDB datasource definition.

Scan a file pattern by selecting template items beginning with a "\$".

Do not select the \$SCRIPTS/mongodb\_unmask\_value.sh item - it is a Guardium reserve item.

If the template item is not specified as part of the Database Instance Directory in the MongoDB datasource definition, the item will be skipped over and not scanned.

Note: For CAS scripts to work, you must enable log in for the MongoDB account on the Mongo DB server. To enable log in, log in as root, run the command **chsh mongod**, and when prompted for new shell, enter /bin/bash.

Note: You can create your own template with multiple file paths for any type of datasource. When creating your own template, we recommend that you use the UNIX/MongoDB as a reference. To create a new template for a MongoDB datasource, you can clone and modify the UNIX/MongoDB template.

Note: MongoDB datasources support SSL server and client/server connections with SSL client certificates. MongoDB connections use a Java driver, instead of a JDBC database connection.

Note: The VA solution for MongoDB clusters can be run on mongos, a primary node and all secondary nodes for replica sets.

## CAS templates - Netezza®

---

### File Ownership

This test checks whether the files are owned and belongs to the correct group according to the definition within the CAS template.

### File Permission

This test checks whether the file permission is properly set according to the definition within the CAS template.

### Scan Log files for errors

This test checks for these events (FATAL, ERROR, DEBUG, ABORT and PANIC) in these two log files. /nz/kit/log/postgres/pg.log and /nz/kit/log/startupsrv/startupsrv.log

## Configuration for Oracle RAC systems

---

This is the required configuration for Oracle RAC systems.

Change guard\_tap.ini on each node installed with S-TAP:

unix\_domain\_socket\_marker=<key>

where <key> value can be found in listener.ora in the IPC protocol definition

Example 1:

If the following is a description in the listener.ora

LISTENER=(DESCRIPTION=(ADDRESS\_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=ORCL)))

Then change the following parameter accordingly

unix\_domain\_socket\_marker=ORCL

Example 2:

In the case where there is more than one IPC line in listener.ora, use a common denominator of all the key LISTENER=(DESCRIPTION=(ADDRESS\_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER)))) LISTENER\_SCAN1=(DESCRIPTION=(ADDRESS\_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER\_SCAN1)))) LISTENER\_SCAN2=(DESCRIPTION=(ADDRESS\_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER\_SCAN2)))) LISTENER\_SCAN3=(DESCRIPTION=(ADDRESS\_LIST=(ADDRESS=(PROTOCOL=IPC)(KEY=LISTENER\_SCAN3))))

Guardium uses a string search in the path so LISTENER will work for all four and should be used in this case:

unix\_domain\_socket\_marker=LISTENER

## CAS templates - PostgreSQL

---

Note: It is very important that PostgreSQL\_BIN and PostgreSQL\_DATA environment variables are defined correctly. An invalid setting causes other CAS assessment tests not to work properly or at all.

### File Ownership

This test checks whether the files are owned and belongs to the correct group according to the definition within the CAS template.

### File Permission

This test checks whether the file permission is properly set according to the definition within the CAS template.

### PostgreSQL\_BIN environment variable defined

This test check if the \$PostgreSQL\_BIN environment variable is defined in your database server. This variable need to be defined under the root account for UNIX/Linux or you can add to .profile for root login. For Windows OS, it needed to be defined for the Administrator login. For Red Hat Linux®, PostgreSQL BIN folder is usually in /usr/bin. For Solaris, it is usually something like /data/postgres/postgres/8.3-community/bin/64. Setting this environment variable is very important as other assessment tests relied on the location of this folder.

### PostgreSQL\_DATA environment variable defined

This test check if the \$PostgreSQL\_DATA environment variable is defined in your database server. This variable need to be defined under the root account for UNIX/Linux or you can add to .profile for root login. For Windows OS, it needed to be defined for the Administrator login. For Red Hat Linux, the default for DATA folder is usually in /var/lib/pgsql/data. For Solaris, there is no consistent location. Setting this environment variable is very important as other assessment tests relied on the location of this folder to find the correct configuration files.

## CAS templates - SQL Server

---

### OS Script

Designates an OS script to run. Output from the script is stored in the Guardium database. This can be either a shell/batch script to be run, or a set of commands that could be entered on the command.

### Registry Variable

Search Windows registry for specific key value that are required by security assessments test.

## CAS templates - Sybase

---

#### OS Script

Designates an OS script to run. Must begin with the variable \$SCRIPTS, which refers to the scripts directory beneath the CAS home directory, and identify the script to run, e.g., \$HOME/sybase\_sysdevice\_type\_test.sh. The script itself must, of course, reside in the CAS \$SCRIPTS directory. Output from the script is stored in the Guardium database to be used by security assessments. This can be either a shell/batch script to be run, or a set of commands that could be entered on the command line. Because of the fickle nature of Java's parsing it is suggested that any but the simplest commands be put into a script rather than run directly. On UNIX the script is run in the environment of the OS user entered. Three environment variables will be defined for the run environment which the user could use in writing scripts: \$UCAS is the DB username, \$PCAS is the DB password, and \$ICAS is the DB instance name. For Windows these three values will be appended as the last three arguments to the batch file execution. For example, if you had an OS Script template %SCRIPTS%\MyScript.bat my-arg1 my-arg2, then %3, %4 and %5 would be the DB username, password, and instance name respectively.

#### File

Designates a file to be tracked and monitored by security assessments. The path to the file can be absolute, or relative to the \$SYBASE variable. The value of the \$SYBASE variable is the value you set in the Database Instance Directory field of the Datasource Definition panel. This is assumed to name a single file. Environment variables from the OS user environment can be used in the file name and will be expanded. For example, \$HOME/START.sh will name the startup script in the Sybase user's home directory.

#### File Pattern

Designates a group of files to be tracked and monitored by security assessments. The path to the files can be absolute, or relative to the \$SYBASE variable. The value of the \$SYBASE variable is the value you set in the Database Instance Directory field of the Datasource Definition panel. A .. in the path indicates one or more directories between the portion of the path before it and the portion of the path after it. A .+ in the path indicates exactly one directory between the portion of the path before it and the portion of the path after it. For example: \$SYBASE/../\*dat" This is just a short-hand for creating many single file identifications from a single identification string, a file pattern. A file pattern can be viewed as a series of regular expressions separated by /'s. A file is matched if each element of its full path can be matched by one of the regular expressions in order. If an element of the pattern is an environment variable, it is expanded before the match begins. If .. is one of the elements of the pattern, it will match zero or more directory levels. For example, /usr/local/..foo will match /usr/local/foo and /usr/local/gunk/junk/bunk/foo. Using more than one .. element in a file pattern should not be necessary and is discouraged because it makes the pattern very slow to expand. Because of the confusion with its use in regular expressions |cannot be used as a separator as it might be in Windows.

Additionally, the Guardium UNIX/Sybase Assessment : UNX - SYBASE set includes the following templates :

#### Scan log files for errors

This test monitors for errors in Sybase log files.

#### sysdevice Owner is sysbase

This test monitors for ownership of sysdevice.

#### File ownership

This test monitors file ownership, and changes thereto, of Sybase files.

#### File permissions

This test monitors file permissions, and changes thereto, of Sybase files.

## CAS templates - Teradata

---

#### File ownership

This test checks whether the files are owned and belongs to the correct group according to the definition within the CAS template.

#### File permission

This test checks whether the file permission is properly set according to the definition within the CAS template.

#### Aster Data

Aster Data was acquired by Teradata in 2011, typically used for data warehousing and analytic application (OLAP). Aster Data created a framework called SQL-MapReduce that allows the Structured Query Language (SQL) to be used with Map Reduce. Aster Data is most often associated with clickstream kinds of applications.

An Aster nCluster includes a Queen Node Group, a Worker Node Group, and a Loader Node Group. A CAS agent is installed on all three node groups.

A security assessment should be created to execute all tests on the queen node. All database connections for Aster Data go through the queen node only.

Testing on worker and loader nodes are only required when performing CAS tests (File permission and File ownership).

Privilege tests loop through all the databases in a given instance.

When running VA tests that require CAS access, and filling in the CAS datasource configuration choices, specify the username that Aster is installed under for Database Instance Account. This username typically is called beehive.

For Database Instance Directory, this is the home directory of the beehive user. The default typically is /home/beehive.

When running VA tests that are do not use CAS, the customer should create their datasource, pointing to the QUEEN node within the cluster.

When running VA tests that are CAS dependent, if the node you are testing is one of the worker, then you would have to setup "Custom URL" in the datasource to point to the Queen node as that is how it is listening.

#### Example

Host Name/IP = Worker.guard.xxx.xxx..com or 1xx.1xx.111.111 (This is the actual worker host even though worker is not listening to this. CAS needs this so it can send and receive data from the Worker's node)

Port = 2046 or whatever the port used.

Database = beehive

Custom URL= jdbc:ncluster://aster6q:2406/beehive (This JDBC example shows that we are actually connecting to the aster6q which is the queen node on port 2406 and beehive database)

Database instance account = beehive

Database instance directory = /home/beehive

## Working with CAS templates

This section describes how to maintain CAS templates and template sets.

### Define a Template/Template Set

- Create a New Template Set
- Modify a Template Set
- Clone a Template Set
- Delete a Template Set

### Create a New Template Set

1. Open the CAS Configuration Navigator by clicking Harden > Configuration Change Control (CAS Application) > CAS Template Set Configuration.
2. Click New to open the Monitored Item Template Definitions panel.
3. Select OS Type.
4. Select DB Type. If the template set does not require any specific DB type then select N\_A as the DB Type.
5. Enter a unique name for Template Set Name.  
Note: Template Set Names over 128 characters will be truncated
6. Click Apply to save the CAS Template Set Definition.
7. To add items to the new template set, click Add to Set and see [Define a Template Set Item](#).

### Finding the Guardium CAS Panel

Access to CAS Configuration Functions, by default, is restricted to the admin user and to users who have been assigned the CAS role.

Click Harden. The list of CAS functions is listed within the Configuration Change Control (CAS Application) header.

### Opening the CAS Configuration Navigator

The CAS Configuration Navigator panel is the starting point for creating or modifying CAS Template Sets.

Open the CAS Configuration Navigator panel by clicking Harden > Configuration Change Control (CAS Application) > CAS Template Set Configuration.

The list can be filtered by OS type and DB type.

### Modify a Template Set

Use the CAS Configuration Navigator panel to modify an existing CAS template set. Once a template set is in use on any CAS host, the modifications that you can make to that template set are limited. You will be able to make minor changes to various elements of the definition, but you will not be able to add or remove templates.

1. Open the CAS Configuration Navigator panel by clicking Harden > Configuration Change Control (CAS Application) > CAS Template Set Configuration.
2. Filter the template set list by OS Type or DB Type.
3. Select the Template Set that you want to modify and click Modify to open the CAS Template Set Definition pane.
4. Make your changes and click Apply to save them.

### Clone a Template Set

1. Open the CAS Configuration Navigator panel by clicking Harden > Configuration Change Control (CAS Application) > CAS Template Set Configuration.
2. Filter the template set list by OS Type or DB Type.
3. Select the Template Set that you want to clone and click Clone to open the CAS Template Set Definition panel.
4. Once cloned, modify the clone to suit your needs.

Note: Predefined templates cannot be edited. They have the same restrictions as those that are in use by a CAS host. To make changes, clone it, then edit the cloned copy as needed.

### Delete a Template Set

1. Open the CAS Configuration Navigator panel by clicking Harden > Configuration Change Control (CAS Application) > CAS Template Set Configuration.
2. Filter the template set list by OS Type or DB Type.
3. Select the Template Set that you want to delete and click Delete.

### Define a Template Set Item

Once a template set is in use on any CAS host, the modifications that you can make to that template set are limited. You will be able to make minor changes to various elements of the definition, but you will not be able to add or remove templates.

- Create a New Template Set Item
- Modify a Template Set Item
- Delete a Template Set Item

## Create a New Template Set Item

1. Open the CAS Configuration Navigator panel by clicking Harden > Configuration Change Control (CAS Application) > CAS Template Set Configuration.
2. Click New to open the Monitored Item Template Definitions panel.
3. Enter in a Template Set Name, select an OS Type and DB Type, and click Apply.
4. Click Add To Set to create a new item.

## Modify a Template Set Item

1. Open the CAS Configuration Navigator panel by clicking Harden > Configuration Change Control (CAS Application) > CAS Template Set Configuration.
2. Filter the template set list by OS Type or DB Type.
3. Select the Template Set that you want to modify and click Modify to open the CAS Template Set Definition panel.
4. Select the items you want to modify, and click Edit Selected.... Make your desired changes and click Apply to save them.

## Delete a Template Set Item

1. Open the CAS Configuration Navigator panel by clicking Harden > Configuration Change Control (CAS Application) > CAS Template Set Configuration.
2. Filter the template set list by OS Type or DB Type.
3. Select the Template Set that you want to modify and click Modify to open the CAS Template Set Definition panel.
4. Select the items you want to delete, and click Delete Selected.

## CAS Item Template Definition Pane

| Component        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OS Type          | The operating system type: Windows or UNIX. You can change this selection when the template set is empty, but you cannot change it if the template set contains one or more items.                                                                                                                                                                                                                                                                                                         |
| DB Type          | The database type (Oracle, MS-Sql, DB2®, Sybase, Informix®, etc.) or N/A for an operating system template set. You can change this selection when the template set is empty but you cannot change it if the template set contains one or more items.                                                                                                                                                                                                                                       |
| Description      | An optional name for the item used in reports and to identify the item in other CAS panels (the CAS Template Set Definition for example). If omitted, the item name defaults to the file name or pattern, variable name, or script (as appropriate for the type).                                                                                                                                                                                                                          |
| Type             | One of the following: SQL Query, OS Script, Environment Variable, Registry Variable, Registry Variable Pattern, File, and File Pattern.<br><br>See Template and Audit Types for further information.<br><br>Note: If being used with CAS-based assessment tests this must be of type OS Script.                                                                                                                                                                                            |
| Content          | Type dependent text defining the specific item to monitor, or how to generate it.<br><br>See Template and Audit Types for further information.<br><br>Note: For an OS script CAS will wait for a script to complete. To limit the time allowed for an OS script to run and allowing CAS to terminate the script, use the <b>cas_command_wait</b> guard_tap.ini parameter. The default wait time is 300 seconds or 5 minutes. When changing this parameter there is no need to restart CAS. |
| Permission Limit | For File and File Pattern Type only.<br><br>Used for UNIX only - the permissions that this file should not exceed.                                                                                                                                                                                                                                                                                                                                                                         |
| File Owner       | For File and File Pattern Type only. The owner of the file(s).                                                                                                                                                                                                                                                                                                                                                                                                                             |
| File Group       | For File and File Pattern Type only. The group owner of the file(s).                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Period           | The maximum interval between tests, specified as a number of minutes(m), hours(h), or days(d). Data becomes available after the initial period is realized and up to and before the next period begins.                                                                                                                                                                                                                                                                                    |
| Keep Data        | If selected, a copy of the actual data is saved with each change. For example: for a file item, a copy of the file is saved. If selected, but the size of the raw data for the item is greater than the Raw Data Limit configured for this CAS host, no data will be saved.                                                                                                                                                                                                                |
| Use MD5          | Indicates whether or not an additional comparison is done by calculating a checksum of the raw data using the MD5 algorithm. Computing the MD5 checksum is time consuming for large character objects. However, it is a better indicator of change than just the size. The default is not to use MD5. If MD5 is used, but the size of the raw data is greater than the MD5 Size Limit configured for the CAS host, the MD5 calculation and comparison will be skipped.                     |
| Enabled          | Selected by default; indicates whether or not the item will be checked for changes.                                                                                                                                                                                                                                                                                                                                                                                                        |

## Template and Audit Types

| Type                 | Description                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SQL Query            | The content should be a valid SQL statement. The result returned by the statement will be compared to the result returned the last time the query was run. The query will be run with the parameters specified in the datasource that is being used: username, password, DB port, and so forth. Care should be taken when filling out these parameters in the datasource or the query will fail to return a result. |
| OS Script            | The content can be a valid command line entry, or the name of a file containing an OS executable script. The script is executed in the environment of the OS user specified in the Database Instance Account field of the datasource definition.                                                                                                                                                                    |
| Environment Variable | The content should name an environment variable that is defined in the context of the OS user specified in the Database Instance Account field of the datasource definition.                                                                                                                                                                                                                                        |

| Type                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Registry Variable         | The content is interpreted as the path to a variable in the Windows Registry of the host. The value found on that path is compared to the value found the last time the path was traced.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Registry Variable Pattern | <p>The content is a sequence of regular expressions that is used to match the components of paths in the Windows Registry. The pattern is used to develop registry variable type monitored items which will be treated as described previously.</p> <p>The regular expressions are joined by / so that the pattern resembles a registry path. The more familiar   character cannot be used, since that is a special character in the syntax of Java™ regular expressions. If a / is needed in one of the regular expressions, it must be escaped with a \ . (e.g. U/235 would be used to match U/235).</p> <p>The pattern .. can be used to match zero or more components within a path. For example, HKLM\Software/../buzz will match HKLM\Software\buzz, or HKLM\Software\one\two\three\buzz. This type of pattern can lead to a computationally expensive registry search, so use it carefully.</p> <p>Other than these exceptions, the regular expressions follow the syntax of Java regular expressions.</p> |
| File                      | The content is interpreted as an absolute file path on the host. The characteristics of the file found on the path will be compared to the characteristic found the last time the path was traced. The path may include environment variables which will be expanded in the context of the OS user specified in the datasource. The path may also begin with a substitution variable, like "\$SYBASE_HOME", which will be replaced by the value entered in the Database Instance Directory field of the datasource definition.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| File Pattern              | The content is a sequence of regular expressions that is used to match the components of file paths and to generate File type monitored items. The regular expressions are joined by / so that the pattern resembles an actual file path. As with registry patterns, the   cannot be used for Windows files because of the regular expression syntax. If the pattern begins with ?: on a Windows machine, the pattern match will be started on each of the drives of a multi-drive machine. The ... construction described with registry patterns can also be carefully used in a file pattern. Environment variables from the context of the OS user can be used in a file pattern and will be expanded before the expansion of the regular expressions.                                                                                                                                                                                                                                                         |

## Configuration Auditing System APIs

CAS includes a robust set of GuardAPIs and REST APIs that you can use to manage hosts, template items, and template sets outside of the Guardium UI. For more information about the APIs, see [Configuration Auditing System APIs](#).

## CAS hosts

A Configuration Auditing System (CAS) host configuration defines one or more CAS instances.

After you define one or more CAS template sets, and install CAS on a database server, you are ready to configure CAS on that host. A CAS host configuration defines one or more CAS instances. Each CAS instance specifies a CAS template set, and defines any parameters that are needed to connect to the database. Each database server on which CAS is installed has a single CAS host configuration, which typically contains multiple CAS instances. For example, one CAS instance to monitor operating system items, and additional CAS instances to monitor individual database instances.

- Define a CAS Instance
- Modify a CAS Instance
- Delete a CAS Instance
- Disable a CAS Instance

## Define a CAS Instance

1. Open the CAS Configuration Navigator by clicking Harden > Configuration Change Control (CAS Application) > CAS Host Configuration. The menu lists all database servers where CAS is installed and this host is connected to the Guardium® system.

2. Filter by the OS Type or DB Type to find the host that you want to work with.
  3. Highlight the host that you want to modify and click Modify.
  4. Select a Template Set from the menu.
- Note: You cannot define a CAS Instance if the host is offline or on a secondary Guardium system for the host.

5. Click Add Datasource to open the Select datasource window.

Note: If no compatible datasource is available for this template set on this host, click  to open the Create datasource window and add a datasource.

6. Select the data source that you want to add to the template set, and click Save to add it to the template set.

## Finding the Guardium CAS Pane

Access to CAS Configuration Functions is restricted to the admin and users who are assigned the CAS role.

Click Harden. All of the CAS functions are listed within the Configuration Change Control (CAS Application) header.

## Open the CAS Configuration Navigator

The CAS Configuration Navigator page is the starting point for creating or modifying CAS Hosts.

Open the CAS Configuration Navigator page by clicking Harden > Configuration Change Control (CAS Application) > CAS Host Configuration.

## Modify a CAS Instance

1. Open the CAS Configuration Navigator.
2. Filter by the OS Type or DB Type to find the instance that you want to work with.
3. Highlight the host to modify and click Modify.

A list of defined CAS instances that are associated with the selected host displays with the following information and editing options:

Table 1. Modify a CAS Instance

| Component                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disable/Enable Instance Icon | Click the Disable Instance icon to disable or enable the CAS instance                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Delete Instance Icon         | Click the Delete Instance icon to delete the CAS instance                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Datasource                   | Identifies the data source that is used by the instance. To edit the data source definition, click Datasource to open the Datasource Definition pane.                                                                                                                                                                                                                                                                                                                                                    |
| Template Set                 | Identifies the CAS template set used by the instance. To view or modify the template set definition, click the link to open the Monitored Item Template Definitions pane.<br><br>For more information, see <a href="#">Working with CAS templates</a> .                                                                                                                                                                                                                                                  |
| Monitored Items              | A count of items currently monitored by the instance. Click this link to open the Monitored Items Definitions pane, which displays the list of all items that are currently monitored.<br><br>For more information, see <a href="#">View Monitored Item Lists</a> .<br>Note: Up to 10,000 monitored items are viewable for reports regardless of the number of monitored items that are defined. To view more items when the number of monitored items approaches this limit, define multiple instances. |

## Delete a CAS Instance

1. Open the CAS Configuration Navigator
2. Filter by the OS Type or DB Type to find the instance that you want to work with.
3. Click Delete Instance to delete a CAS instance. All collected change data is also deleted.

## Disable a CAS Instance

1. Open the CAS Configuration Navigator.
2. Filter by OS Type or DB Type to find the instance that you want to work with.
3. Highlight the host that you want to modify and click Modify, or double-click to open the Host Instance Definitions pane.
4. Click Disable Instance to disable a CAS Instance. Change data is not collected until the instance is enabled again when you click the icon.

## View Monitored Item Lists

In the Host Instance Definitions pane, click a Monitored Items link to view the complete list of items monitored in the Monitored Items Definitions pane. The following table describes the components in the Monitored Items Definitions pane for this Host Configuration.

All the monitored items refer to raw data, a character object on the host, the result of an SQL query, the output of an OS script, or the contents of a file. The size of that character object is computed. If the item is a file, then the permissions, owner, group, and last modified time are also checked. If any of the objects changed since the last time the item was checked, the change is noted.

Table 2. View Monitored Item Lists

| Component  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Select Box | Check the Select Box if you'd like to edit a monitored item individually or as a group. Double-click any monitored item to edit that item.                                                                                                                                                                                                                                                                                                                              |
| Item       | The name of the monitored item from the description in the CAS Item Template Definition pane.                                                                                                                                                                                                                                                                                                                                                                           |
| Type       | One of the following types: <ul style="list-style-type: none"> <li>• OS Script or SQL Script: The actual text or the path to an operating system or SQL script, whose output will be compared with the output produced the next time that it runs.</li> <li>• File or File Pattern: A specific file or a pattern to identify a set of files.</li> <li>• Environment Variable or Registry Variable: An environment variable or a (Windows) registry variable.</li> </ul> |
| Period     | The average interval between tests, which are specified as a number of seconds (s), minutes (m), hours (h), or days (d).                                                                                                                                                                                                                                                                                                                                                |
| Keep Data  | If marked, a copy of the actual data is saved with each change. For example, for a file item, a copy of the file is saved. If marked, but the size of the raw data for the item is greater than the Raw Data Limit configured for this CAS host, no data is saved.                                                                                                                                                                                                      |
| Use MD5    | Indicates whether the comparison is done by calculating a checksum of the raw data by using the MD5 algorithm. Computing the MD5 checksum is time-consuming for large character objects. However, it is a better indicator of change than just the size. The default is not to use MD5. If MD5 is used, but the size of the raw data is greater than the MD5 Size Limit configured for the CAS host, the MD5 calculation and comparison is skipped.                     |

## Configuration Auditing System APIs

CAS includes a robust set of GuardAPIs and REST APIs that you can use to manage hosts, template items, and template sets outside of the Guardium UI. For more information about the APIs, see [Configuration Auditing System APIs](#).

## CAS reporting

This section describes Configuration Auditing System (CAS) reporting.

The admin user has access to all query builders and default reports. The admin role allows access to the default CAS reports, but not to the CAS query builders. The CAS role allows access to both the default CAS reports and the query builders.

## Accessing the Query-Report Builder

See [Using the Query-Report Builder](#).

CAS domains are described in [Domains, Entities, and Attributes](#).

CAS predefined reports are described in [Predefined admin reports](#).

## Accessing Default CAS Reports

View the default reports related to CAS by clicking Harden > Reports.

## CAS status

To open the Configuration Auditing System Status page, browse to Harden > Reports > CAS Status

Displays the CAS status, and the status of each CAS instance for each database server that is configured as the active Guardium® host and where CAS is installed and running.

Hover your mouse over the status lights to display the status text.

| Component                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CAS System Status indicator light | Indicates whether CAS is actively running on the Guardium system.<br>Red - CAS is not running on this Guardium system.<br>Green - CAS is active on this Guardium system.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| CAS agent status indicator lights | Indicate whether the individual CAS agent is connected to a Guardium system. Identify each CAS agent by referencing the IP address that appears before the row of status indicator lights.<br>Red - Either the host, the CAS agent, or both are offline or unreachable.<br>Green - Host and CAS agent are online.<br>Yellow - The Guardium system is a secondary for the CAS host.                                                                                                                                                                                                                               |
| Reset                             | Reset the CAS agent on this monitored system, which stops and restarts the CAS agent on the database server.<br>Note: Reset also resets checkpoint files; allowing for a fresh start and rescan of files from scratch.                                                                                                                                                                                                                                                                                                                                                                                           |
| Delete (X)                        | Remove this monitored system from CAS and delete the data on the Guardium system that is associated with the CAS client.<br>Delete is unavailable if the CAS agent is running on this system. To delete the monitored system, stop the CAS agent first. For more information, see <a href="#">Stopping and starting the CAS agent</a> .                                                                                                                                                                                                                                                                          |
| Red/Yellow/Green light            | Indicates the status of a CAS instance on the monitored system. If the owning monitored system status is red (indicating that the CAS agent is offline), ignore this set of status lights.<br>Red - The instance is disabled.<br>Green - The instance is enabled and online, and its configuration is synchronized with the Guardium system configuration.<br>Yellow - The instance is enabled, but the instance configuration on the Guardium system does not match the instance configuration on the monitored system (that is, the instance is updated in Guardium, but the monitored system is not updated). |
| Refresh                           | Update the status of all servers in the list. Refresh does not stop or restart CAS on a database server. Refresh checks only the connection between CAS on the Guardium system and CAS on each database server.                                                                                                                                                                                                                                                                                                                                                                                                  |

Note: The TAP\_IP entry in the guard\_tap.ini file is required. If TAP\_IP is missing CAS does not start, and an error message is logged in the log file on the CAS client.

## Stopping and starting the CAS agent

Several situations exist where you might need to stop or start the CAS agent on a monitored system.

Stopping CAS on a UNIX host

1. Edit the file /etc/inittab.
2. Find the CAS respawn line:

```
, cas:2345:respawn:/usr/local/guardium/guard_stap/cas/bin/run_wrapper.sh /usr/local/guardium/guard_stap/cas/bin
```

3. Insert a number sign (#) in the first character position to comment out the line.
4. Save the file.
5. Enter the following commands and note the PID of each listed process.

```
init -q
ps -er | grep cas
```

6. For each process, issue the following command,

```
kill -9 <pid>
```

7. In the Configuration Auditing System Status window, make sure that the status light for this CAS host is red, and that the Remove button is enabled. If needed, click Remove to remove data from this CAS host from the Guardium system internal database.

Starting CAS on a UNIX host

Restart the CAS agent only if it was stopped by editing the /etc/inittab file as described in [Stopping CAS on a UNIX host](#).

1. Edit the file /etc/inittab.

2. Find the respawn line:

```
, #cas:2345:respawn:/usr/local/guardium/guard_stap/cas/bin/run_wrapper.sh /usr/local/guardium/guard_stap/cas/bin
```

3. Remove the # in the first character position to uncomment the line.

Note: Depending on your operating system, the comment character might be different.

4. Save the file.

5. Enter the following command to restart the CAS agent, **init -q**.

Starting and Stopping CAS on a Windows Host

On Windows, CAS runs as a system service.

1. In the Windows Services window, highlight the Configuration Auditing System Client item.

2. Select either Start or Stop from the Action menu.

## License information for Guardium Vulnerability Assessment

The license information describes the purchase options for Guardium Vulnerability Assessment. It also describes how to measure the license for Guardium Vulnerability Assessment and perform scans on nonproduction, failover, disaster recovery, and other environments.

Note: This License Guide is intended to provide only supplementary information to assist you in deploying the Programs you have licensed from IBM within your purchased entitlement. Your license agreement (such as the IBM International Program License Agreement (IPLA) or equivalent and its transaction documents, including the License Information for IBM Security Guardium Vulnerability Assessment is the sole and complete agreement between you and IBM regarding use of the Program.

## Purchasing options for Guardium Vulnerability Assessment

Guardium Vulnerability Assessment can be purchased by using the stand-alone part numbers or as part of the Guardium Package Software.

This licensing guide is specific to Guardium Vulnerability Assessment stand-alone parts. For more information about Guardium Package Software, see [Guardium Package Software License Guide](#).

## Measuring licensing for Guardium Vulnerability Assessment

Resource entitlements convert to managed virtual servers (MVS). You must obtain sufficient entitlements based on the quantity of managed virtual server (MVS) scanned by the program.

The entitlements apply no matter where client data resides, provided the users account for the correct number of MVS to cover the servers, where the Guardium Vulnerability Assessment is scanning your data sources.

A managed virtual Server (MVS) can be one of two types of servers:

- A physical computer composed of processing units, memory, and input/output capabilities that execute requested procedures, commands, or applications for one or more users or client devices. If racks, blade enclosures, or other similar equipments are used, each separable physical device (for example, a blade or a rack-mounted device) that has the required components is considered a separate server.
- A virtual server that is either a virtual machine created by partitioning the resources of a physical server or an unpartitioned physical server.

For on-prem (noncloud) data sources, any server with a unique IP address or hostname is counted as an MVS. The unique IP address can be a physical IP address or a virtual IP address based on the database type and deployment architecture.

The following scenarios explain the behavior of Guardium Vulnerability Assessment. When Guardium Vulnerability Assessment runs an assessment scan against:

- A multinode or high availability data source (for example, Oracle RAC and Teradata), each node that is associated with a unique IP address (physical or virtual) or a unique host must be counted as a separate MVS for entitlement. See [Example 2: Counting multinode systems](#) for more information.
- A Database Management System (DBMS) comprising multiple databases, each node or an instance associated with a unique IP address (physical or virtual) or a unique host must be counted as a separate MVS for entitlement. See [Example 4: Counting multiple databases across multiple instances \(non z/OS\)](#) for more information.
- A cloud database or cloud warehouse, each node, instance, and a database must be counted as a separate MVS for entitlement. See [Example 6: Counting databases on cloud DBaaS](#) and [Example 7: Counting databases on Snowflake environment](#) for more information.

## Performing Guardium Vulnerability Assessment scans on nonproduction, failover, disaster recovery, and other environments

Nonproduction activities for Guardium Vulnerability Assessment are activities other than running scans to harden the environment, and these activities are independent of the environment type.

When you run scans on nonproduction environments such as development and testing, these environments are considered as production use for Guardium Vulnerability Assessment, and need sufficient entitlements.

Similarly, when you run scans on other types of environments, such as failover and disaster recovery, these environments are also considered as production use, and need sufficient entitlements.

In high availability (HA) and disaster recovery (DR) scenarios; for example, Oracle DataGuard, if the standby databases are not scanned by Guardium Vulnerability Assessment, no entitlement is needed. However, if the standby databases are scanned by Guardium Vulnerability Assessment, even if they are cold" or "warm" standby, entitlement is needed to cover these databases.

The database systems that are sharing the workload and IP address for scaling compute and storage purposes; for example, Veritas InfoScale or VMWare VMotion capabilities do not require a separate scan for hardening purposes. So, these databases do not need additional entitlements.

- [Example scenarios](#)

The following section lists the example scenarios for calculating entitlements.

## Example scenarios

The following section lists the example scenarios for calculating entitlements.

Note: These examples are not exhaustive in terms of different database deployment architectures.

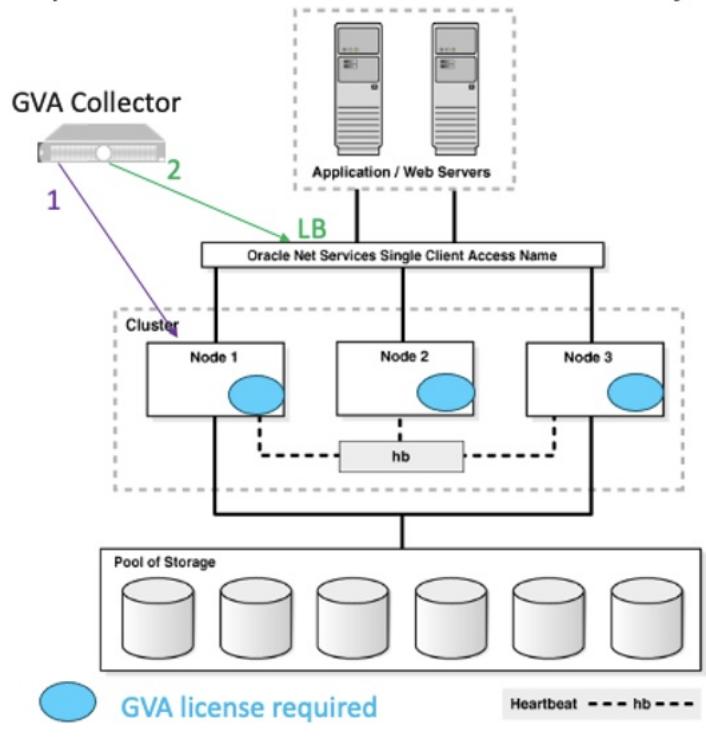
### Example 1: Counting MVS (Managed Virtual Server) by hostname/IP

If you use Guardium Vulnerability Assessment to scan 100 database servers, each with a unique IP address or hostname, you need entitlements that support 100 MVS.

If you use Guardium Vulnerability Assessment to scan more than 100 database servers with unique IP address or hostname, you need an additional entitlements that support 100 MVS.

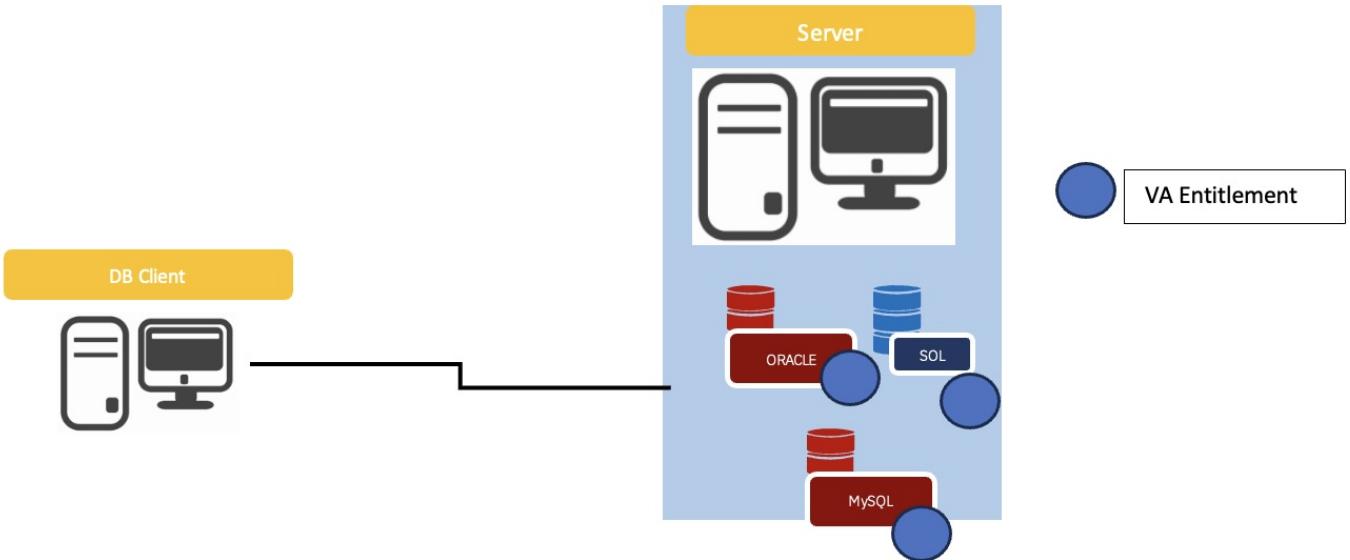
### Example 2: Counting multinode systems

If you have an on-prem database system with 3 nodes for high availability as shown in the following figure, you require 3 MVS of Guardium Vulnerability Assessment.



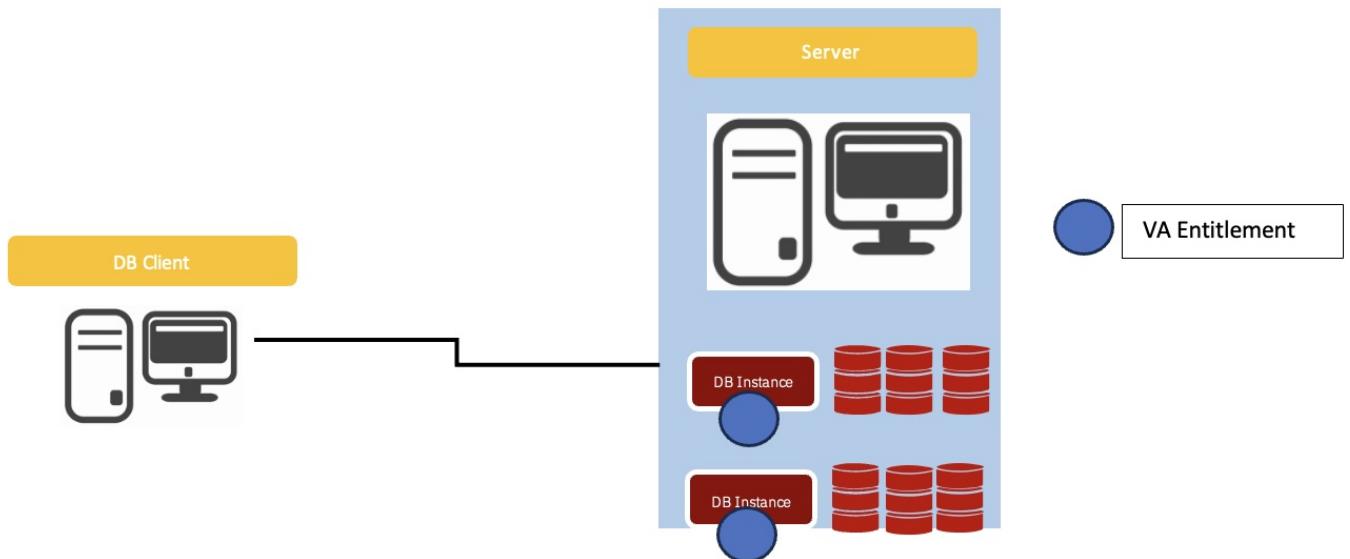
### Example 3: Counting DB systems deployed by different DB vendors

If you have an on-prem server with 3 different DBs deployed, you require 3 MVS of Guardium Vulnerability Assessment regardless of the IP configuration of these database instances.



#### Example 4: Counting multiple databases across multiple instances (non z/OS)

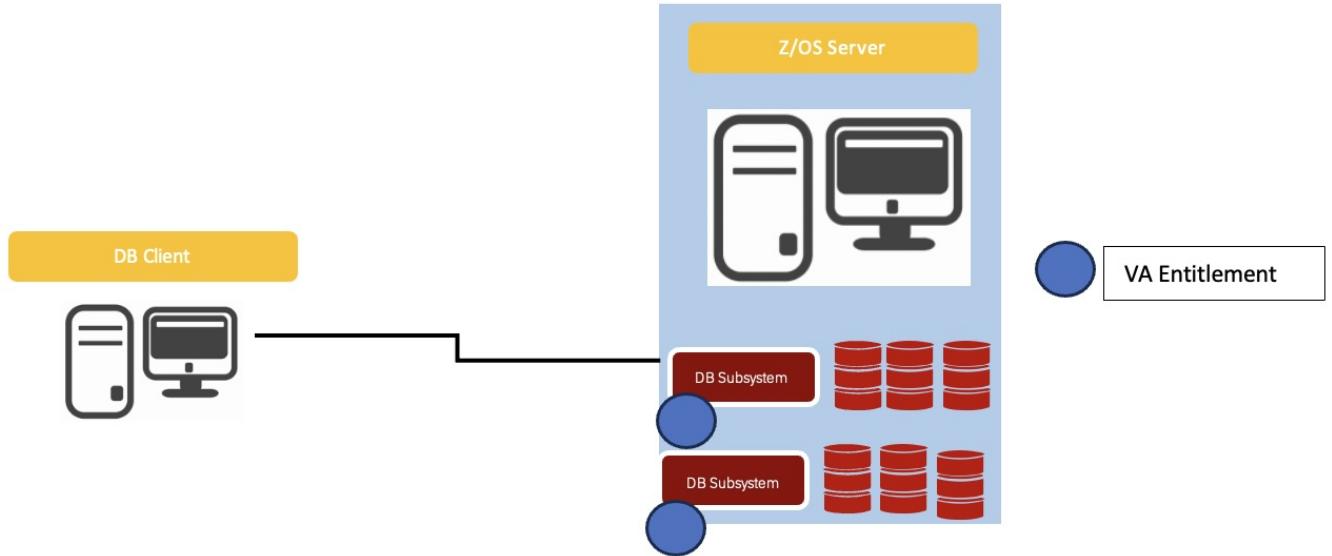
If you have an on-prem DBMS with 2 instances deployed and each of the DB instance has 3 databases, you need 2 MVS of Guardium Vulnerability Assessment.



#### Example 5: Counting Db2 running on z/OS

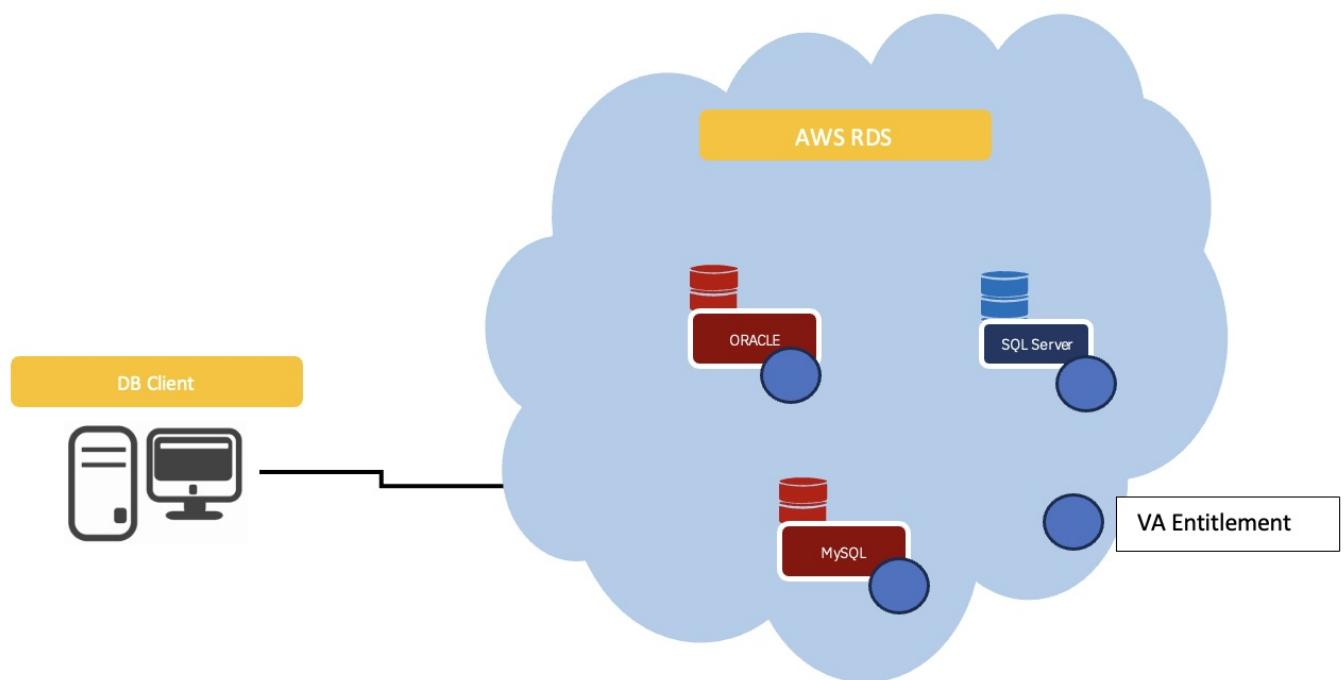
If you use Guardium Vulnerability Assessment to scan 2 Db2 for z/OS subsystems, you need an entitlement that supports 2 MVS.

Note: A subsystem on Db2 z/OS is similar to an instance of Db2 running on Linux, UNIX, and Windows systems. The subsystem provides a separate Db2 environment and configuration. Guardium Vulnerability Assessment has two separate part numbers; one for Linux, UNIX, and Windows (LUW) and another for Db2 for z/OS. So, ensure that you use the correct part number for scanning these systems.



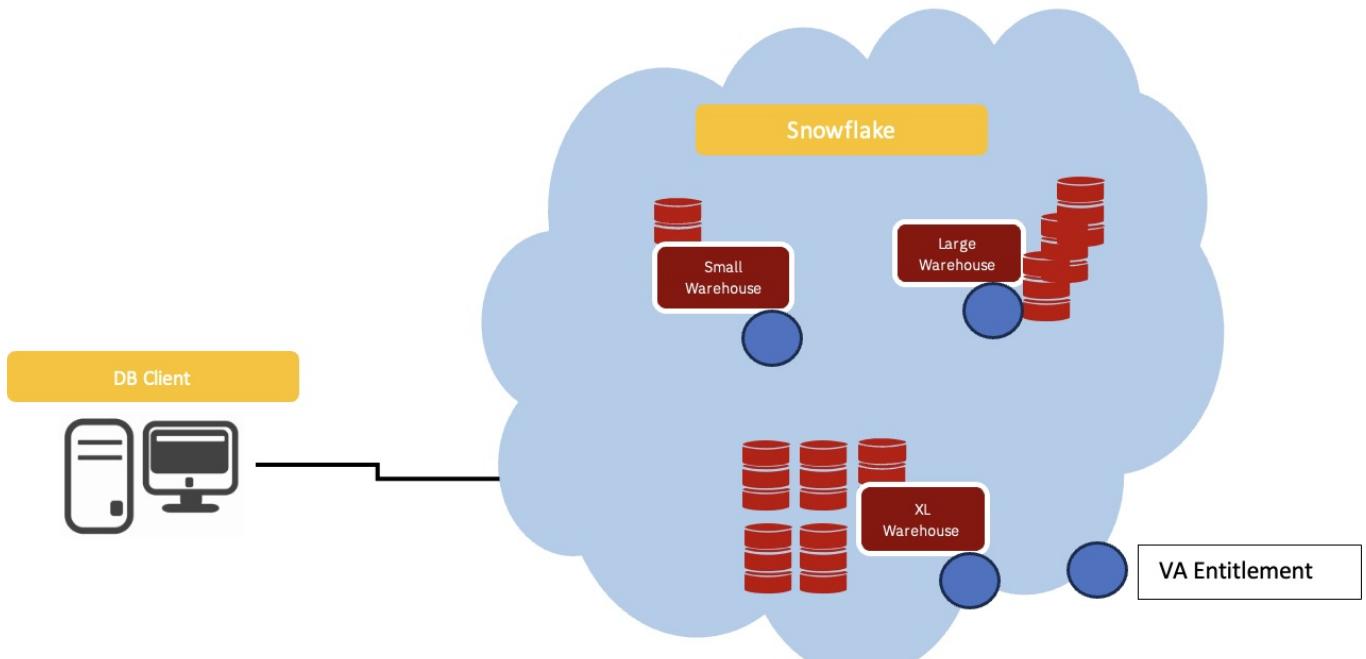
### Example 6: Counting databases on cloud DBaaS

If you use Guardium Vulnerability Assessment to scan 3 databases in your AWS Relational Database Service (RDS) environment, each with a unique IP address or hostname, you need 3 MVS of Guardium Vulnerability Assessment regardless of the compute power allocated to each of these databases.



### Example 7: Counting databases on Snowflake environment

If you are use Guardium Vulnerability Assessment to scan 3 instances in your Snowflake environment, you need 3 MVS of Guardium Vulnerability Assessment regardless of the instance size.



The exact number of Resource Value Units (RVUs) for all these scenarios can be calculated by using the VUE Table 103A mentioned in [License Information](#).

## Configuring your Guardium system

You can configure several aspects of your Guardium system to enable you to meet your business goals effectively and efficiently.

- [\*\*System Configuration\*\*](#)  
Most of the information on the System Configuration panel is set by using the CLI at installation time.
- [\*\*Managing data: archive, restore, aggregation, and system backup\*\*](#)  
Establish data retention practices; control activity volume; manage scheduling of data archive and purge, and monthly backups.
- [\*\*Internet Protocol modes\*\*](#)  
Configure Guardium® to run in a traditional IPv4-only environment, an IPv6-only environment, or in *dual mode* where the system supports both IPv4 and IPv6 addresses.
- [\*\*Network mirroring methods \(SPAN, N-TAP\) and related inspection engines\*\*](#)  
This configuration is used in cases where an S-TAP cannot be installed in the host where the database instances to be monitored are run. Instead, you can direct a copy of the network traffic that goes to the host running the database servers, to a Guardium collector. This method only captures network traffic, not local traffic within the database server host. The limitations are listed further on in this section. IBM strongly encourages you to use an S-TAP instead.
- [\*\*Configuring inspection engines\*\*](#)  
An inspection engine extracts SQL from network packets; compiles parse trees that identify sentences, requests, commands, objects, and fields; and logs detailed information about that traffic to an internal database.
- [\*\*Configuring the Guardium portal\*\*](#)  
From the Guardium Portal page, you can reset the port for the Guardium appliance web server, import SSL certificates, and configure authentication for your Guardium system users.
- [\*\*Managing the TLS version\*\*](#)  
Use APIs to manage TLS 1.2 and TLS 1.3 protocols for your appliances, S-TAP agents, CAS and GIM clients. As you update your Guardium system to Guardium 12.0, you can enable TLS 1.3 and disable TLS 1.2.
- [\*\*Global profile\*\*](#)  
The Global Profile page defines defaults that apply to all users.
- [\*\*Configuring the alerter\*\*](#)  
Configure and activate the alerter to send email messages, SNMP traps, and alert-related Syslog messages.
- [\*\*Facility and priority of syslog messages\*\*](#)  
The facility and priority of messages configured in the Guardium syslog can impact how they are consumed by the Security Incident Event Manager (SIEM).
- [\*\*Anomaly Detection\*\*](#)  
The Anomaly Detection process runs every polling interval to create and save, but not send, correlation alert notifications that are based on an alert's query.
- [\*\*Session Inference\*\*](#)  
Session Inference checks for open sessions that have not been active for a specified period of time, and marks them as closed.
- [\*\*Allow \(approve\) S-TAP connection to Guardium \(S-TAP certification\)\*\*](#)  
Use this function to control the specific S-TAP hosts whose clients are allowed ("approved") to access the Guardium system.
- [\*\*IP to Hostname Aliasing\*\*](#)  
The IP-to-Hostname Aliasing function accesses the Domain Name System (DNS) server to define hostname aliases for client and server IP addresses.
- [\*\*Configure Permission to Socket connection\*\*](#)  
This topic applies to Custom Alerting Classes.

## System Configuration

Most of the information on the System Configuration panel is set by using the CLI at installation time.

For instructions on how to configure the system, or to modify any other System Configuration settings, see [Modify the System Configuration](#).

There must be a valid license to use various functions within the appliance. When a license is entered after the system starts, a restart of the GUI is needed.

## About System Shared Secret

The Guardium® administrator defines the system shared secret in the System Configuration window. The system shared secret is used for two general purposes:

- To sign and encrypt files for export or archive, and for importing or restoring data exports and data archives.
- To establish secure communications between Central Managers and managed units.

If you are using Central Management and/or aggregation, you must set the System Shared Secret for all related systems to the same value.

The system shared secret value is null at installation time. Depending on a company's security practices, it may be necessary to change the system shared secret on a periodic basis. Each appliance maintains a shared secret keys file, containing an historical record of all shared secrets defined on that appliance. The same system thus will have no problem at a later date decrypting information that has been encrypted on that system.

When information is exported or archived from one system, and imported or restored on another, the latter must have access to the shared secret used by the former. For these cases, there are CLI commands that can be used to export the system shared secrets from one Guardium system, and import them on another.

See the following commands in the CLI appendix:

- **aggregator backup keys file**
- **aggregator restore keys file**

## Modifying the System Configuration

1. Click **Setup > Tools and Views > System** to open System Configuration.
2. Make your changes.
3. Click **Apply** to save the updated system configuration.

Note: The applied changes do not take effect until the Guardium system is restarted. After you apply configuration changes, click **Restart** to stop and restart the system.

Table 1. System Configuration Panel Reference

| Field or Control         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unique Global Identifier | This value is used for collation and aggregation of data. The default value is a unique value that is derived from the MAC address of the machine. Do not change this value after the system begins monitoring operations.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| System Shared Secret     | <p>Any value that you enter here is not displayed. Each character you type is masked.</p> <p>The system shared secret is used for archive/restore operations, and for Central Management and aggregation operations. When used, its value must be the same for all units that will communicate. This value is null at installation time, and can change over time.</p> <p>The system shared secret is used:</p> <ul style="list-style-type: none"><li>• When secure connections are being established between a Central Manager and a managed unit.</li><li>• When an aggregated unit signs and encrypts data for export to the aggregator.</li><li>• When any unit signs and encrypts data for archiving.</li><li>• When an aggregator imports data from an aggregated unit.</li><li>• When any unit restores archived data.</li></ul> <p>Depending on your company's security practices, you might be required to change the system shared secret from time to time. Because the shared secret can change, each system maintains a shared secret keys file, containing an historical record of all shared secrets defined on that system. This allows an exported (or archived) file from a system with an older shared secret to be imported (or restored) by a system on which that same shared secret has been replaced with a newer one.</p> <p><b>Caution:</b> When used, be sure to save the shared secret value in a safe location. If you lose the value, you will not be able to access archived data.</p> |
| Retype Secret            | When you enter or change the system shared secret, retype the new value a second time. Any value that you enter here is not displayed. Each character you type is displayed as an asterisk.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| License Key              | <p>The license key is inserted in the configuration during installation. Do not modify this field unless you are instructed to do so by Technical Support. You might need to paste a new product key here if optional components are being added.</p> <p>If you install a new product key on the central management unit, when you click <b>Apply</b>, you will receive a warning message that reads: <b>Warning: changing the license on a Central Management Unit requires refreshing all managed units.</b> After you click <b>OK</b> to close the message window, you must click <b>Apply</b> a second time to install the new product key. You will know that the new license has been installed when you receive the message: <b>Data successfully saved.</b></p> <p>If you install a new product key on a Central Management Unit, you might get a warning that states the license applied to the CM must be refreshed on the managed unit. This requires a refresh done from the Central Manager and is done by pressing the refresh icon from the Central Manager to each of the collectors listed.</p> <p>License entitles user to access products and the corresponding features.</p> <p>License can be appended or overridden.</p> <p>Active license is stored in <b>LICENSE_KEY</b> in <b>ADMINCONSOLE_PARAMETER</b></p> <p>Product types DAM; FAM; VA</p> <p>Edition for product types: Express; Standard; Advanced</p>                                                                                 |
| Number of Datasources    | If a limited license is applied, the maximum number of datasources permitted per datasource license is displayed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Metered Scans Left       | If a limited license is applied, the number of vulnerability assessment scans permitted (datasource metering) per metering license is displayed. Each time a vulnerability assessment is triggered, the scan counter decreases by one.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| License valid until      | If a limited license is applied, a fixed date when the license will be disabled is displayed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Field or Control                                                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| # of Licenses                                                                                      | This value indicates the number of licenses remaining.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Note: Configure Network Address, Secondary Management Interface and Routing settings using the CLI | These settings cannot be configured through the GUI and appear grayed-out on the System Configuration user interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| System Hostname                                                                                    | The resolvable host name for the Guardium system. This name must match the DNS host name for the primary System IP Address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Domain                                                                                             | The name of the DNS domain on which the Guardium system resides.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| System IP Address                                                                                  | The primary IP address that users and S-TAP or CAS agents use to connect to the Guardium system. It is assigned to the network interface labeled ETH0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| SubNet Mask                                                                                        | The subnet mask for the primary System IP Address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Hardware (MAC) Address                                                                             | The MAC address for the primary network interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| System IP Address (Secondary)                                                                      | <p>Optional: A port can also be configured to team with the primary interface in order to provide high-availability failover IP teaming. Alternatively, a port on the device can be configured as a secondary management interface with a different IP address, network mask, and gateway from the primary.</p> <p>These two options are mutually exclusive.</p> <p>There are two different, and mutually exclusive, kinds of secondary management connections, both controlled by options to the same CLI command:</p> <p>Bonding or teaming</p> <p>Turns the primary interface and another specified network interface card (NIC) into a bonded pair with standby failover. To implement this option, use the CLI command <b>store network interface high-availability on &lt;nic&gt;</b>, where nic is an available NIC.</p> <p>Secondary interface</p> <p>Allows the GUI and CLI to be accessible from another NIC in the Guardium system. To implement this option, use the CLI command <b>store network interface secondary on &lt;nic&gt; &lt;ip&gt; &lt;mask&gt; &lt;gateway&gt;</b> to specify the secondary NIC, its IP address and network mask, and optionally a gateway.</p> <p>BOTH physical and VM systems have the same capabilities. Dependent on the number of NICs installed on the Guardium system or VM.</p> <p>To display the network interfaces installed on the unit, use the <b>show network interface inventory</b> CLI command. For example:</p> <pre>show network interface inventory Current network card configuration: Device   Mac Address   Member of ----- eno3    08:94:EF:28:AA:F9   br2 eno1    08:94:EF:28:AA:F7   eno2    08:94:EF:28:AA:F8   br1 eno4    08:94:EF:28:AA:FA   br3 ens2f0   00:21:5E:E2:9F:0C   br7 ens2f1   00:21:5E:E2:9F:0E   br8 ens1f1   40:F2:E9:1E:40:18   br6 ens1f0   40:F2:E9:1E:40:19   br5 ens3f1   90:E2:BA:D8:50:3D   br10 ens3f0   90:E2:BA:D8:50:3C   br9</pre> <p>Note: The "Member of" will show which NICs are in a bond pair, if a bonding exists.<br/>To locate the eth connectors on your appliance, use the <b>show network interface port</b> CLI command, which will blink the orange light on that port, 20 times. For example:</p> <pre>guard14.xyz.com&gt; sho net int port 3</pre> <p>The orange light on port eth5 now blinks 20 times.</p> <p><b>Note:</b> The secondary IP address and its associated port are NOT related to the high availability feature, which provides fail-over support via IP Teaming for the primary connection. For more information about the high-availability option, see the <b>store network interface</b> commands in the CLI Appendix.</p> |
| SubNet Mask (Secondary)                                                                            | Optional. The subnet mask for the secondary System IP Address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Default Route/ Secondary Route                                                                     | The IP address of the default router for the system./ The IP address of the Secondary Router.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Primary Resolver Secondary Resolver Tertiary Resolver                                              | The IP address for the Primary Resolver (DNS) is required. The secondary and tertiary are optional.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Test Connection                                                                                    | Click Test Connection to test the connection to the corresponding DNS (Domain Name System) server. This only tests that there is access to port 53 (DNS) on the specified host. It does not verify that this is a working DNS server. You will receive a message box indicating if the DNS server responded.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Stop                                                                                               | Click Stop to shut down the system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Restart                                                                                            | Click Restart to stop and then restart the system. You will be prompted to confirm the action.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Apply                                                                                              | Click Apply to save the changes. The changes are applied the next time the system restarts.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## Managing data: archive, restore, aggregation, and system backup

Establish data retention practices; control activity volume; manage scheduling of data archive and purge, and monthly backups.

- [Planning archiving, storage capacity, and scheduling](#)

Learn about archiving and purging, and capacity and scheduling planning, so you can configure archiving and purging on your system.

- [Managing stored data](#)  
Typically, no more than one or two months worth of audit data is stored on an appliance (or as little as a few days), to save disk space and maintain performance. However, auditors might require to keep audit data available for a few years. Guardium® provides the mechanism to archive audit data in chunks of one day and store them on a remote location. Configure the archive process during implementation to run daily. Configure archive and purge as part of your overall data management policy. Learn how to archive, and export and import data from collectors to aggregators.
- [Exporting \(files\) results](#)  
CSV, CEF, and PDF files can be created by workflow processes. This function exports all such files that are on the Guardium system to the target system you specify.
- [Viewing days whose data was not archived or exported](#)  
The predefined report **Days that are not archived or exported** shows the days whose data remains on the appliance, and will not be purged based on the Guardium system settings.
- [Data and Result catalogs](#)  
Each Guardium system can have both a Data catalog and a Result catalog. The catalogs list all archive files that were created on the server. Each time the system archives data or results, one entry is added to the relevant catalog. Each archive file is tracked, so that it can be retrieved and restored.
- [Data aggregation](#)  
Collect and merge information from multiple Guardium units into a single Guardium Aggregation appliance to offload the reporting and analysis function from the collectors, while also providing a consolidated view of the data from multiple collectors.
- [Purging data](#)  
Data that has been successfully archived should be purged from the Guardium appliance to maintain the disk space. Configure and schedule the purge mechanism during the implementation stage to run nightly: to purge data that is older than a specified number of days.
- [Configuring system backup](#)  
System backups store all the necessary data and configuration values to restore a Guardium Server. Configure and schedule regular system backups during the implementation stage.
- [Restoring a Guardium system](#)  
Each type of guardium system (collectors, aggregators, and central manager) have different purposes and store data in different ways. Use the appropriate recovery strategies for each system type. The recovery strategy that is used also depends on whether the system that must be recovered is a stand-alone appliance or is used with other systems.
- [Enabling SSH key pairs for data archive, data export, data mart](#)  
You can use SSH key pairs for authentication, instead of passwords, for archiving and exporting results, archiving data, and exporting data marts.
- [Transferring data to a remote host by using SSH key pairs for authentication](#)  
You can archive and export results, archive data, and export data marts with SSH key pairs for authentication, instead of usernames and passwords.
- [Configuring external storage](#)  
Archive files can be sent using SCP or FTP protocol, or to a configured external storage system (Amazon S3, EMC Centera, Tivoli Storage Manager, IBM COS, and IBM Cloud). You can define a single archiving configuration for each Guardium system.

## Planning archiving, storage capacity, and scheduling

Learn about archiving and purging, and capacity and scheduling planning, so you can configure archiving and purging on your system.

### Archiving and Purging

Archiving and purging data on a regular basis is essential for the health of your Guardium® system. Archive preserves information for future use. Purge frees up space and speeds up access operations on the internal database. For the best performance, archive and purge all data that is not needed. For example, if you only need three months of data on the Guardium appliance, archive and purge all data that is older than 90 days.

The Guardium archive function creates signed, encrypted files that cannot be tampered with. Archive files are transferred and stored on external systems such as file servers or storage systems. For more information about the encryption used for archives, see the *File backup cipher* section of [Cipher suites](#).

If both archive and purge are scheduled, purge runs after archive.

Data that was archived on a collector can be restored either on another collector or an aggregator server. Data that was archived on an aggregator cannot be restored on a collector.

The export, archive, and purge functions can work on the same data, but not the same date ranges. For example, you may want to export and archive all information older than one day and purge all information older than one month, thereby always leaving one month of data on the sending unit.

### Data retention

Data retention policies vary widely from depending on your system and your needs. Factors to consider include:

- Required retention time
- Amount of stored data/day
- Disk size

You could decide to keep seven days of data on the collectors, and to maintain the data on the aggregators for a much longer period.

For disaster recovery: keep a rolling two-weeks worth of daily archives from the managed collectors.

Note: If you have stand-alone collectors, maintain daily archives according to your data retention policy.

For historical investigation or auditing purposes, maintain daily archives from the collectors for the period that is required by your auditing or corporate data-retention policies.

### Archiving from collectors versus aggregators

Archive is required if you need to store more data than your disk allows. You can archive from either collectors or aggregators. There are advantages and disadvantages to both. It comes down to what works best for you. After data is successfully archived, it can be purged from the Guardium appliance.

Audit data is stored in normalized form in an internal database of a Guardium system. The audit data that changes constantly is referred as dynamic data. The audit data that stays relatively constant is referred as static data. The user login time is a good example of dynamic data. It is unique for every user, for each login. Username is an example of static data. It stays the same for every login of this user to the database.

Archives from an aggregator are full archives: static and dynamic data, which simplifies the archive restore process.

Archives from collectors use an incremental archive strategy. The dynamic audit data is archived when it is observed. Static audit data is archived only when the data is observed for the first time. This incremental approach reduces the size of archive files dramatically. The tradeoff is that a single archive file might not contain all of the audit data that you want to restore. To compensate for this tradeoff, the archive process generates a full (not incremental) archive file the first time the archive process runs, and then the first day of every month. For example, to restore 28 June, either restore 1 June through 28 June, or restore 28 June and 1 July.

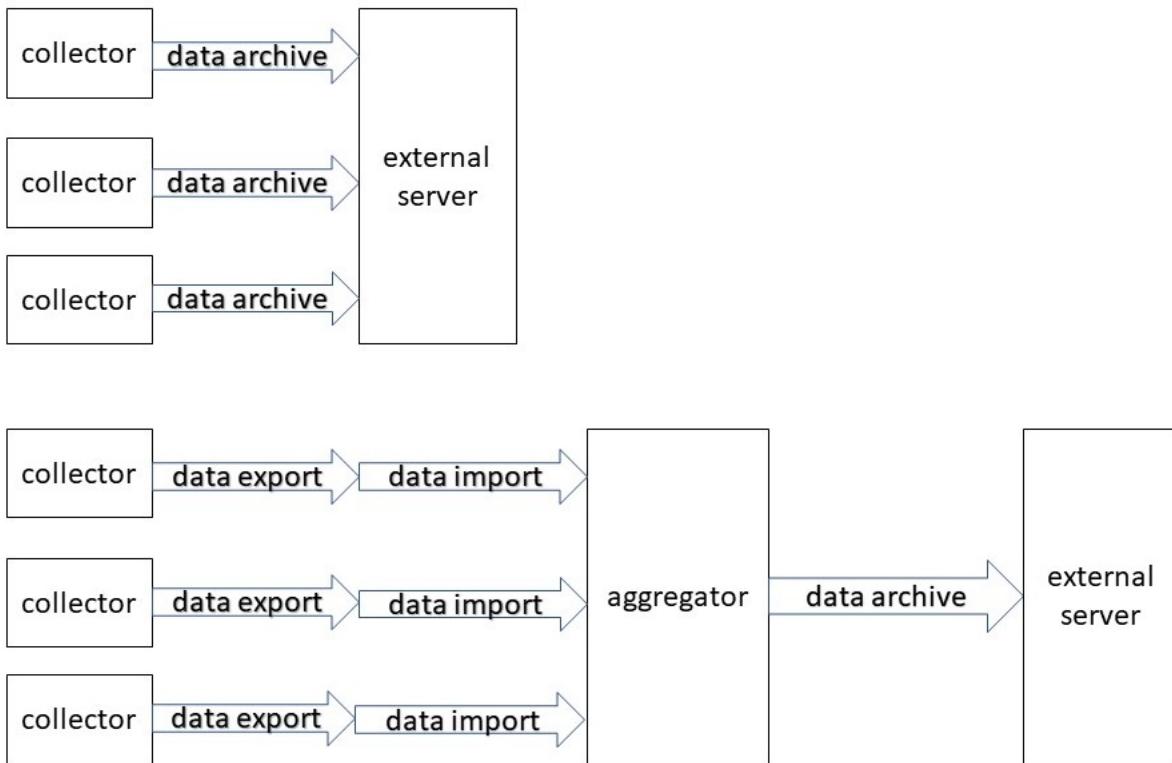
Archiving on the collectors:

- Incremental daily information for both static and dynamic data.
- Static data is archived in full during the archive on the first day of each month.
- Archiving data from the original source.
- Less usage of long-term storage.
- To restore data for specific day: restore data for all days of that month up to the target day.
- Collector's archive file can be restored directly into aggregator.

Archiving on the aggregators:

- Incremental daily information for dynamic data.
- Static data is archived in full daily.
- Verify that imports are complete before starting the archive; otherwise, some data can be missing in the archive.
- More usage of long-term storage (static data is included every day).
- Faster restore: need to restore only one file for the specific target day.

Figure 1. Archiving from collectors to an external server, or exporting to an aggregator and archiving from the aggregator



## Storage capacity

The following are only estimates of backup and archive file sizes for auxiliary storage capacity planning purposes. The actual sizes vary depending on the volume and granularity of the database activity that is logged on the Guardium collectors, and the retention period of the backup files.

Daily Archives:

- Collector: approximately 40 MB (privileged user monitoring) to 1 GB (Comprehensive monitoring with full details logged on all traffic).
- Aggregator: a rough multiple of the number of collectors, for example, Number of collectors multiplied by 40 MB.

Monthly System backups, assuming a 50% full database on 600 GB disk size:

Note: The backup gets roughly a 1:8 compression for the backup file.

- Collector: 7 – 10 GB
- Aggregator: 16 – 20 GB
- Central Manager (no aggregation): < 1 GB

Results Archives: Depends on the number and frequency of audit processes implemented.

The amount of data kept online is constrained by the size of the database on each Guardium system. The Purge process helps to manage how much data is kept online. Purge is coordinated with the Daily Archive so that all data is retained as required. Keep the minimum amount of data necessary on your Guardium system to avoid filling up the database and to maintain database performance.

Guardium recommends 15 days for the collector and 30 days for the aggregator. The actual length depends on how much data is recorded (for example, numbers of S-TAPs, policy rules, and collectors).

## Control activity volume

Controlling the volume of activity monitored (on the database server) and logged (on the collector) helps to:

- Reduce network usage.
- Reduce the Guardium system's database disk consumption.
- Improves the overall capacity and performance of the system.

This control is primarily achieved in the policy rules, and in the inspection engine configuration, by using these guidelines:

- Avoid specifying port ranges in inspection engines.
- Identify all trusted applications and batch programs (these programs generally generate the bulk of the database activity). If possible, ignore, or skip their activity by using the Ignore S-TAP Session or Skip Logging actions.
- Unless necessary, avoid the Log Full Details action in your policies.
- If possible, use the Selective Audit policy (with the Ignore S-TAP session rules) to minimize network traffic.
- If no extrusion rules are used, for example, result sets are not examined. Consider using the Ignore Responses per Session action to eliminate result sets being sent to the Guardium system.
- Establish a process to periodically review and update policy rules, including groups to accommodate new databases and applications.
- Establish a process to periodically monitor SQL Errors and provide to the DBA and Application development teams for remediation.

## Scheduling

Default schedule times are supplied when the unit is built and these can be amended accordingly. The Data Management tasks should be scheduled at less busy times, for example, overnight. They should be spaced out so as not to overlap (for example, one task should complete before the next one starts.)

In a typical scenario, data older than one day is archived, and data older than two days is ignored. It's critical that the data import completes before the data archive starts, to capture the data that is one day old.

If the Data Archive runs BEFORE the Data Imports from other Collector(s)/Aggregator(s), then the Archive does NOT contain the imported data that should be archived. For example: Data Archive runs at 00:30 and Data Import runs at 06:00. In this scenario, when the Archive runs, yesterday's data is not yet present in the system because the Import of yesterday's data has not occurred. By scheduling Data Archive AFTER the Data Import(s) have finished, the Archive contains yesterday's data.

Another issue that can arise if the archive is scheduled too early in the day: suppose the export on one of your collectors failed, and you successfully rerun the export in the morning. You would need to manually rerun all processes related to this data: import to process the file, possibly rerun your audit processes, rerun the archive since the archive file didn't have data from one of the collectors. But when the archive is scheduled for 7PM, you don't need to rerun any tasks.

The timing of the archive is flexible as long as it is later in the day, and it finishes on the same day.

It's recommended to run import and audit tasks early in the morning, so that you have current reports available at the start of the workday.

The following tables provide a summary of the key schedules to be configured on your Guardium systems.

Use the Aggregation/Archive log to record the time and status of these processes to assist with adjusting your scheduling times.

Table 1. Typical collector schedule

| Function                                   | Schedule                                                                            |
|--------------------------------------------|-------------------------------------------------------------------------------------|
| Data export (to the Aggregators) and purge | Daily: 12:30 AM<br>Purge is initially set to 15 days.                               |
| Data Archive (stand-alone)                 | Daily: 03:00 AM                                                                     |
| Audit/Workflow jobs                        | Daily: 03:00 AM (for stand-alone systems)                                           |
| CSV/CEF export to the SCP/FTP Server       | Daily: 05:00 AM, if configured in the Audit jobs and after the audit jobs complete. |
| IP-to-Hostname Aliasing                    | Daily: 06:00 AM                                                                     |
| Policy Reinstallation                      | Daily: 11:00 PM                                                                     |
| System backups                             | Monthly: First Sunday of each month at 7:00 AM                                      |

Table 2. Typical aggregator schedule

| Function                             | Schedule                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Archive and Purge               | Daily: 7:00 PM<br>Purge is initially set to 60 days.<br>Archives are scheduled during a quiet period after the following tasks are complete: <ul style="list-style-type: none"><li>• The daily import of data from the collectors, so that the data is included in the archive. This must include data from the collectors in different time zones.</li><li>• Any audit processes are run.</li></ul> |
| Data Import (from the Collectors)    | Daily 2:30 AM                                                                                                                                                                                                                                                                                                                                                                                        |
| Audit/Workflow jobs                  | Daily: 03:30 AM                                                                                                                                                                                                                                                                                                                                                                                      |
| CSV/CEF export to the SCP/FTP Server | Daily: 05:15 AM, if configured in the Audit jobs, and after the audit jobs complete.                                                                                                                                                                                                                                                                                                                 |
| IP-to-Hostname Aliasing              | Daily: 06:00 AM                                                                                                                                                                                                                                                                                                                                                                                      |
| System backups                       | Monthly: First Sunday of each month at 7:00 AM                                                                                                                                                                                                                                                                                                                                                       |

Note: Avoid scheduling before 12:15 AM to avoid any conflicts with the internal start-of-day processing on each Guardium system.

## Managing stored data

Typically, no more than one or two months worth of audit data is stored on an appliance (or as little as a few days), to save disk space and maintain performance. However, auditors might require to keep audit data available for a few years. Guardium® provides the mechanism to archive audit data in chunks of one day and store them on a remote location. Configure the archive process during implementation to run daily. Configure archive and purge as part of your overall data management policy. Learn how to archive, and export and import data from collectors to aggregators.

- [Configure data archive](#)

*Data Archive* backs up the audit data that Guardium captured, for a specified date, to another location. Typically, data is archived for the previous day, which ensures that if there is a catastrophe, only the data of that day is lost. This practice also saves disk space and boosts appliance performance. Configure and schedule the archive mechanism during the implementation stage to run nightly: to archive the last day's data.

- [Archiving \(audit\) results](#)

The results archive includes: reports, assessment tests, entity audit trail, privacy sets, classification processes, and the view and sign-off trails and the accumulated comments from workflow processes. Use Archived results for compliance purposes.

- [Restoring archived data](#)

You can restore archived data files to review historical data, and run reports or investigations.

## Configure data archive

*Data Archive* backs up the audit data that Guardium captured, for a specified date, to another location. Typically, data is archived for the previous day, which ensures that if there is a catastrophe, only the data of that day is lost. This practice also saves disk space and boosts appliance performance. Configure and schedule the archive mechanism during the implementation stage to run nightly: to archive the last day's data.

### About this task

Archive and purge are enabled independently of each other, and the ages at which data is archived and purged are configured independently.

*Data Archive* files can be used for data restoration for forensic purposes when data for a limited number of days needs to be restored. Restoring archive data does not override the existing data: you can restore data on an appliance that already has data, but you can't restore data on the same unit if data for that day still exists.

In an aggregated environment, data can be archived from the collector, from the aggregator, or from both locations. Most commonly, the data is archived only once, and the location from where it is archived varies depending on your requirements.

The audit data is stored in a normalized way in an internal database of an appliance. The audit data that changes constantly is referred as dynamic data, and the audit data that stays relatively constant is referred as static data. For example, profile data is static and audit data is dynamic.

To save space on storage servers, Guardium uses an incremental archive strategy. The dynamic audit data is archived when it is observed. Static audit data is archived only when the data is observed for the first time. This incremental approach reduces the size of archive files dramatically. The tradeoff is that a single archive file might not contain all of the audit data that is needed to be restored back to the appliance. To compensate for this tradeoff, the archive process generates a full (not incremental) archive file the first time the archive process runs, and then again the first day of every month. If you want to have a full archive for the next archive run, use this CLI command: **store archive\_static\_table=on**. After that run, the parameter switches back to be **off**. To check if the static data will be archived in the next run, run the CLI command: **show archive\_static\_table**.

The data archive is usually set to archive data older than one day and ignore data older than two days. In this scenario, each run archives only the data from the previous day.

Guardium's archive function creates signed, encrypted files that cannot be tampered with. DO NOT change the names of the generated archive files. The archive and restore operations depend on the file names that are created during the archiving process.

Archive uses the system shared secret to create encrypted data files. Before information encrypted on one system can be restored on another, the target restore system must have the shared secret that was used on the archiving system when the file was created. Data can be restored on the same unit type it was archived from: collector data on a collector, aggregator data on an aggregator.

The archive data file name format is one of:

- <day of data>-<Guardium system name>-w<time of zip>-d<execution date>.dbdump.enc
- <day of data>-<Guardium system name>-w<time of zip>-d<execution date>.agg.<sql ver>tar.gc.enc

Note: The archive and restore operations depend on the file names generated during the archiving process. DO NOT change the names of archived files.

## Procedure

1. Go to [Manage](#) > [Data Management](#) > [Data Archive](#).
2. To archive, check the Archive checkbox. More fields display in the Configuration page.
3. For Archive data older than, enter a value and select a unit of time from the menu. For example, to archive data from yesterday, enter the value 1, and select Day(s) from the menu.
4. In Ignore data older than enter the time interval to archive. For example, to archive one day's data, enter 2. Any value that is specified here must be greater than the Archive data older than value. If you leave this field blank, you archive data for **all days** older than the value specified in Archive data older than. If you archive daily and purge data older than 30 days, you archive each day of data 30 times (before it is purged on the 31st day).
5. Check the Archive Values checkbox to include values from SQL strings in the archived data. If this box is cleared, values are replaced with question mark characters on the archive (and hence the values are not available following a restore operation).
6. Select a Protocols option, and enter the appropriate information. Depending on how your Guardium system is configured, one or more of these buttons might not be available. For a description of how to configure the archive and backup storage methods, see [Configuring external storage](#) or [File Handling CLI Commands](#).
7. Optional: Use the Scheduling section to define a schedule for running this operation regularly.
8. Click Test connection The system attempts to verify the configuration by sending a test data file to that location. If the operation fails, an error message displays and the configuration is not saved.

9. Click Save to save the configuration changes. The system attempts to verify the configuration by sending a test data file to that location. If the operation fails, an error message is displayed and the configuration is not saved.

10. Optional: Click Run Once Now to run the operation now.

## What to do next

---

- Verify that the operation completed successfully. Go to Manage > Reports > Data Management > Aggregation/Archive Log. Each archive operation shows multiple activities. Check that the status of each activity is Succeeded.
- AWS archives only. Check that the files were uploaded:
  - Log in to the AWS Management Console: <http://aws.amazon.com/console/> with your email address and password.
  - Click S3.
  - Click the bucket that you specified in Guardium UI. Verify that the files are there.
- EMC Centera archives only. Check that the files were uploaded to the EMC Centera. You need the name of the files and a ClipID.

## Related concepts

---

- [Viewing days whose data was not archived or exported](#)

## Archiving (audit) results

---

The results archive includes: reports, assessment tests, entity audit trail, privacy sets, classification processes, and the view and sign-off trails and the accumulated comments from workflow processes. Use Archived results for compliance purposes.

## About this task

---

Archiving results is optional: archive results if you need to store more than your disk allows.

An alternative to using the results archive is to save a PDF file from the Audit Process after all users complete the review process.

Guardium's archive function creates signed, encrypted files that cannot be tampered with. DO NOT change the names of the generated archive files. The archive and restore operations depend on the file names that are created during the archiving process. Archive and export activities use the system shared secret to create encrypted data files. Before information encrypted on one system can be restored on another, the restoring system must have the shared secret that was used on the archiving system when the file was created.

The audit process results that must be signed **are not archived** until they are reviewed and signed. Only the Audit Processes configured to be archived are archived. To archive an audit process, select Archive in the Advanced options of the Name and archive section of the Create New Audit Process page.

The results sets can be restored only into an investigation center. You can set up an investigation center by creating a special investigation user account on a Guardium® appliance. See [Investigation center](#).

## Procedure

---

- Go to Manage > Data Management > Results Archive.
- For Archive data older than, enter a value and select a unit of time from the menu. To archive data older than today's data, enter the value 1, and select Day(s) from the menu.
- Use Ignore data older than to control how many days of data are archived. Any value that is specified here must be greater than the Archive data older than value. If you leave this field blank, you archive data for all days older than the value specified in Archive data older than. For example, if you archive daily and purge data older than 30 days, you archive each day of data 30 times (before it is purged on the 31st day).
- Select a Protocols option, and enter the appropriate information. Depending on how your Guardium system is configured, one or more of these buttons might not be available. For a description of how to configure the archive and backup storage methods, see [Configuring external storage](#) or [File Handling CLI Commands](#).
- Optional: Use the Scheduling section to define a schedule for running this operation regularly.
- Click Test connection. The system attempts to verify the configuration by sending a test data file to that location. If the operation fails, an error message appears and the configuration is not saved.
- Optional: Click Run Once Now to run the operation now.

## What to do next

---

- Verify that the operation completed successfully. Go to Manage > Reports > Data Management > Aggregation/Archive Log. Each archive operation shows multiple activities. Check that the status of each activity is Succeeded.

## Related reference

---

- [Archive, export, import, purge, and restore APIs](#)

## Restoring archived data

---

You can restore archived data files to review historical data, and run reports or investigations.

## Before you begin

---

Restore archived data from a collector only to the same collector, an aggregator, or a different collector that is dedicated to investigation that is not part of an aggregation cluster. Data that was archived on an aggregator cannot be restored on a collector.

## About this task

---

Archives are written to an SCP or an FTP host, or to another external storage system. Archived files are restored by retrieving them through the archive catalog. The [Data and Result catalogs](#), on each Guardium system, track archived files. A new record is added to the catalog whenever the appliance archives data or results. The catalog tracks where every archive file is sent so that the archive files can be retrieved and restored with minimal effort at any point in the future. To restore archives, you must copy one or more archive files to the Guardium system on which the data is to be restored.

Each day's data is in a separate file. Depending on how your archive and purge operations are configured, you might have multiple copies of archived data for the same day. For example, you schedule archive to run more than once per day; you click Run Once Now a couple of times; or the archive is scheduled to run and you also click Run Once Now.

Unless you are restoring data from the first archive that was created during the month, you need to restore multiple days of data because of the incremental archive strategy. All information that is needed for a restore operation is archived automatically, the first time that data is archived each month. Use one of these two methods to restore data:

- Restore the first day of the month and all the following days until the target date.
- Restore the target date and then the first day of the following month.

For example, to restore 28 June, either restore 1 June through 28 June, or restore 28 June and 1 July.

Restoring archive files from older versions into newer version appliance is supported for both collector and aggregator archive files. Restoring archive files into different or newly built appliances is supported. However, the "shared secret" used to archive on the original appliance must be the same as on the target appliance.

Restored audit data can be viewed as the regular audit data by using interactive or audit process reports.

- [Restoring archived data on an empty appliance](#)

You can restore archived data to a stand-alone system that has no other audit data on it, and is designated for restoring and reviewing historical data. Use a stand-alone system to avoid interference with current data that is operating.

- [Restoring a few days of recent data](#)

Use this procedure to restore a few days worth of data that was archived from the Guardium system that you are restoring it to.

- [Restoring and viewing audit results in the investigation center](#)

The investigation center is an extension of the aggregators. Investigation users (when defined) can restore results of selected historic dates and perform forensic investigation. After the data is restored, the investigation users can define and view reports by using the standard Guardium UI, only in the scope of the investigated dates.

---

## Restoring archived data on an empty appliance

You can restore archived data to a stand-alone system that has no other audit data on it, and is designated for restoring and reviewing historical data. Use a stand-alone system to avoid interference with current data that is operating.

## Before you begin

---

- Restoring from Tivoli Storage Manager only: A dsm.sys configuration file must be uploaded to the Guardium® system. Use the CLI command: **import tsm config**.
- Restoring from EMC Centera only: a .pea file must be uploaded to the Guardium system, in the Data Archive page.
- If the target restore system is not the system that generated the archive, you must create a location entry in the catalog. Create the entry either with the Catalog Archive ([Data and Result catalogs](#)) or with the GuardAPI ([create\\_entry\\_location](#)). This entry enables the file transfer to the target restore system.
- If the file was encrypted by a different Guardium system, make sure that the system shared secret used by the Guardium system that encrypted the file is available on this system. Otherwise, it cannot decrypt the file. See [About System Shared Secret](#).

## About this task

---

This procedure describes one method of adding a file record to a catalog. You can also move the file entry to the catalog by one of:

- Run [Export catalog entries](#) on the Guardium system where the archive files were created, then run [Import catalog entries](#) on the target Guardium restore system.
- Run [create\\_entry\\_location](#) on the target Guardium restore system, then run [delete\\_entry\\_location](#) on the Guardium system where the archive files were created.

## Procedure

---

1. Go to Manage > Data Management > Catalog Archive.
2. Enter the start and end dates, optionally enter the hostname, and click Search.
3. If the archive files that you want are not in the list, add the entries manually:
  - a. Click Add. The Add Location pane opens.
  - b. Select the Storage System: the type of server that the files are saved on. The fields update accord to the server type. Some might be unavailable.
  - c. Enter values for:
    - File Name: name of archive file that you want to restore, in one of these formats:
      - <day of data>-<Guardium system name>-w<time of zip>-d<execution date>.dbdump.enc
      - <day of data>-<Guardium system name>-w<time of zip>-d<execution date>.agg.<sql ver>tar.gc.enc
    - Host Name: server on which the archive file is located
    - Path: full path to the archive file:
      - Amazon S3: bucket name
      - IBM COS: bucket name
      - EMC Centera: Centera clipID
      - SFTP (Formerly FTP): directory relative to the SFTP account home directory.

- SCP: directory as an absolute path.
  - IBM Cloud: Container
  - Tivoli Storage Manager: path
  - User Name: user with read access to retrieve the archive file.
    - Amazon S3, IBM COS: Access Key ID
    - IBM Cloud: X-Auth-User
  - Password: password for the user.
    - Amazon S3: Secret Access Key
    - IBM COS: Secret Access Key
    - IBM Cloud: X-Auth-Key
  - Retention: number of days to store the data on the target restore system.
4. Click Save.  
 The entry is added to the catalog.
5. Go to [Manage > Data Management > Data Restore](#).  
 The Data Restore Search Criteria window opens.
6. Select From and To dates to specify the time range for which you want data.  
 The Data Restore Search Results pane opens.
7. Optional: To filter the search results, enter the Host Name of the Guardium system from which the archive originated.
8. Click Search.  
 The Data Restore Search Results page opens, showing the records for all archive files from this Guardium system.
9. Optional: To prevent purging of restored data even though it meets the purge requirements on the target restore Guardium system: enter the number of days that you want to retain the restored data on the system in the Don't purge restored data for at least field, and click Apply.
10. Check the Select checkbox for each archive you want to restore.
11. Click Restore.
12. Click Done when you are finished.

## What to do next

Verify that the restore operation status in [Manage > Reports > Data Management > Restored Data](#) is Succeeded.

## Restoring a few days of recent data

Use this procedure to restore a few days worth of data that was archived from the Guardium® system that you are restoring it to.

### Before you begin

- On a Guardium collector, stop the inspection-core process by running CLI command **stop inspection-core**.
- To restore from a TSM (Tivoli Storage Manager) server, upload a dsm.sys configuration to the Guardium system. Use the CLI command: **import tsm config**.
- To restore from an EMC Centera, upload a .pea file to the Guardium system, in the Data Archive page.
- If the target restore system is not the system that generated the archive to be restored, create a location entry in the Catalog Archive ([Data and Result catalogs](#)) or by running the GuardAPI ([create\\_entry\\_location](#)). This information is used to transfer the file to the target restore system.
- If the archive file was created on a different Guardium system, verify that the system shared secret used by the Guardium system that encrypted the file is available on this system. Otherwise, it cannot decrypt the file. See [About System Shared Secret](#).

### About this task

Restoring archived data from a collector to: the same collector; an aggregator; or a different collector that is dedicated to investigation that is not part of an aggregation cluster.

Data cannot be captured during the restore process.

### Procedure

1. Go to [Manage > Data Management > Data Restore](#).  
 The Data Restore Search Criteria window opens.
2. Select From and To dates to specify the time range for which you want data.  
 The Data Restore Search Results pane opens.
3. Optional: To filter the search results, enter the Host Name of the Guardium system from which the archive originated.
4. Click Search.  
 The Data Restore Search Results page opens, showing the records for all archive files from this Guardium system.
5. Optional: To prevent purging of restored data even though it meets the purge requirements on the target restore Guardium system: enter the number of days that you want to retain the restored data on the system in the Don't purge restored data for at least field, and click Apply.
6. Check the Select checkbox for each archive you want to restore.
7. Click Restore.
8. Click Done when you are finished.

## What to do next

Verify that the restore operation status in [Manage > Reports > Data Management > Restored Data](#) is Succeeded.

## Restoring and viewing audit results in the investigation center

The investigation center is an extension of the aggregators. Investigation users (when defined) can restore results of selected historic dates and perform forensic investigation. After the data is restored, the investigation users can define and view reports by using the standard Guardium® UI, only in the scope of the investigated dates.

Each Guardium appliance maintains a catalog of all the data and results archived. The catalog contains information about the archive, its location, and credentials to access them. The catalog is exported from the collectors and merged into a complete catalog on the aggregator as part of the aggregation process. As an investigation user, you select the dates for restore. The results for these dates are uploaded to the investigation center and merged into that investigation user's view. In addition to merging collectors' catalogs through the aggregator, you can export and import catalogs from Manage > Data Management.

## Users and Roles

---

The special investigation role (`inv`) is available in an aggregator. Users with the `inv` role can perform forensic investigations on historic data. Only `inv` users can access the investigation center.

The role `inv` is a special role that connects the user to a separate, investigation-only internal database. It is usually combined with the role user, and in general it is incompatible with all other roles. The Run an Ad-Hoc Audit Process button is available on all report screens for all users except investigation (INV) user.

**Important:** The Last Name of the `inv` user must be one of the three investigation databases: INV\_1, INV\_2, or INV\_3 (case-sensitive). An investigation user uses the same query and report definitions as any other user would. The biggest difference is that the investigation user sees only the data that is uploaded for the investigation database. Multiple investigators can be configured to share an investigation database. Selected data can be restored from archive or viewed from the current database if the data was not purged yet. An investigation user can also restore archived audit process results and view them.

## Investigation context

---

The investigation center supports three concurrent investigation periods, named INV\_1, INV\_2 and INV\_3. Each can hold separate historic data, and provide the means of forensic investigation of that period. When logged in to the investigation center, the last name of the user indicates which investigation database you are viewing.

## Restore audit results

---

In the Audit Process builder, you can specify whether the results of a process are archived or not. Only results of processes marked for archive, and for which all sign-offs are complete, are archived. Results of specific runs are packed, compressed, and stored. The location is recorded in the catalog. These results contain the results, the view, and sign-off trails, and the comments associated with these results. Archived results can be restored to an investigation center.

1. Log in to the Guardium GUI as a user with the `inv` role.
2. Go to Manage > Data Management > Audit Results Restore to open the Restored Data page. Any previously restored results are listed. You can click Discard Data to unmount all previously mounted results.
3. Click Audit Results Restore to open the Results Restore Search Criteria page.
4. Enter the From: date and the To: date for the time period that you want to search.
5. Optionally, enter a Host name, Audit Process, or Run Number to further filter the result set.
6. Click Search to view the result set.
7. From the result set produced, check the Select box of those results you want to restore.
8. Click Restore to restore the selected results. Depending on the number of results to restore, and whether the data sets are local to the system, the restore process can take a long time.
9. You can monitor the progress of the restore process in View Restore Log.

## View Restore Log

---

The restore log provides a view of the Restore of past and current restore attempts that are filtered for the current user.

Go to Manage > Reports > Data Management > My Restore Log to open My Restore Log.

## Viewing Restored Audit Results

---

1. Log in to the Guardium GUI as a user with the `inv` role.
2. Go to Comply > Tools and Views > Audit Results Navigation to open the Audit Process Finder page.
3. From the drop-down list, select a process.
4. Click View to open another window and view the available reports for the audit results.

## Exporting (files) results

---

CSV, CEF, and PDF files can be created by workflow processes. This function exports all such files that are on the Guardium system to the target system you specify.

## About this task

---

Export data file names have the format: <daysequence>-<hostname.domain>-w<run> datestamp>-d<data\_date>.dbdump/TAR

CEF and CSV files that are created by workflow processes can also be written to syslog. When that happens, those files are not available to be exported by the method described here. Access those files in the syslog or by other means.

## Procedure

---

1. Go to Manage > Data Management > Results Export (files)
2. Select the protocol, one of: SCP or SFTP (Formerly FTP).
3. Enter the parameters:

- Host - The IP address or DNS hostname of the host to receive the files.
  - Directory - The target directory on the target destination server. The format depends on the protocol you selected.
    - For SCP - Specify the directory as an absolute path.
    - For SFTP - Specify the directory relative to the SFTP account home directory.
  - Port - Port on the target destination server. The default port for SSH, FTP, and SFTP is 22.
  - User Name - Username for the target destination server. This user must have write or execute permissions for the specified directory.
  - Password - Password for Username on the target destination host.
4. Click Save to save the configuration. The system attempts to verify the configuration by sending a test data file to that location. If the operation fails, it displays an error message. If the test file is transmitted successfully, the Scheduling section becomes active.
5. Optional: Use Scheduling to define a schedule for running this operation regularly.
6. Optional: To export the files now, click Run Once Now.

## What to do next

---

- Verify that the operation completed successfully. Go to [Manage > Reports > Data Management > Aggregation/Archive Log](#). Check that the status of each export activity is Succeeded.

## Related concepts

---

- [Scheduling](#)
- [Global profile](#)

## Related reference

---

- [configure\\_results\\_export](#)

## Viewing days whose data was not archived or exported

---

The predefined report **Days that are not archived or exported** shows the days whose data remains on the appliance, and will not be purged based on the Guardium system settings.

The Data archive and Data export pages have an option Allow purge without exporting or archiving that prevents purge from running before export or archive are complete. To ensure that no data is lost (before it is exported or archived), this option is not selected. However, the Guardium system can end up storing older days of data, due to an export or archive process that failed or was paused. This data can cause or contribute to a long running purge process or too much data on appliances. To maintain a well-running appliance, consider archiving or exporting, and purging the older days.

The report shows the days whose data was not archived or exported and would not be purged based on the current settings of purge process. You can archive or export days on a one-off basis, by using the Archive data older than and Ignore data older than values in the Data archive or Data export pages.

Using the report:

- Archive or export must be scheduled daily on the appliance for the report to work as expected.
- Set the runtime parameters back as far as possible, for example, NOW -48 Month, to identify all older days.
- The report shows days that would not be purged based on the current purge setting and if those days were older than the purge period. This means:
  - Today's date appears in the report even though it is too soon to archive it. You can ignore this date.
  - If Allow purge without exporting or archiving is selected, no data shows in the report because all the data would be purged.

## Data and Result catalogs

---

Each Guardium® system can have both a Data catalog and a Result catalog. The catalogs list all archive files that were created on the server. Each time the system archives data or results, one entry is added to the relevant catalog. Each archive file is tracked, so that it can be retrieved and restored.

## About this task

---

Catalog entries can be transferred between appliances by the following methods:

- Aggregation: Catalog tables are aggregated, which means that the aggregator has the merged catalog of all of its collectors.
- Export Catalog: Use the export function to transfer catalog entries between collectors, or to export a catalog to an external storage.
- Import Catalog: Use the import function to import one or more archive file records that were exported using Export Catalog.
- Data Restore: Each data restore operation contains the data of the archived day, reflected in the catalog entries of that day. When you restore data, the catalog is also updated.
- **[Import catalog entries](#)**  
Perform this task on a target restore server, to import one or more archive files that were created and saved to a backup location.
- **[Export catalog entries](#)**  
Use this task to export catalog entries from the catalog on the Guardium system that created the archive file. The resulting generated file can be imported to the Guardium system on which you want to restore the archives.
- **[Adding, removing, and modifying catalog entries](#)**  
Catalog entries are created each time that the system archives results or data. In time, you might want to modify the records.

## Related reference

---

- [Catalog entry APIs](#)

## Import catalog entries

Perform this task on a target restore server, to import one or more archive files that were created and saved to a backup location.

### About this task

When catalog entries are imported from another system, those entries point to files that have been encrypted by the original system. Before you restore or import any such file, the system shared secret of the originating system (that encrypted the file) must be available on the target import system. You can use the **aggregator backup keys file** and **aggregator restore keys file** CLI commands to copy the shared secrets from one Guardium® system to another.

### Procedure

1. Go to **Manage > Data Management > Catalog Import**.
2. Click **Browse** to locate and select the file.
3. Click **Upload**. You are notified when the operation completes and the definitions that are contained in the file are displayed. Repeat to upload more files.
4. Click the green arrow for each file you want to import, or click **Remove** without **Importing** to remove the uploaded files without importing the contents.

### Related reference

- [Catalog entry APIs](#)

## Export catalog entries

Use this task to export catalog entries from the catalog on the Guardium® system that created the archive file. The resulting generated file can be imported to the Guardium system on which you want to restore the archives.

### Procedure

1. Go to **Manage > Data Management > Catalog Export**.
2. Select a definition type from the Type dropdown list: Data Catalog or Result Catalog.  
The Definitions to Export list is populated with entries of the selected type.
3. Select each entry that you want to export and click **Export**.  
Depending on your browser security settings, you might see a message that asks whether you want to save the file or open it.
4. Choose a target location to save the exported file.

### Related reference

- [Catalog entry APIs](#)

## Adding, removing, and modifying catalog entries

Catalog entries are created each time that the system archives results or data. In time, you might want to modify the records.

### About this task

Take the scenario where the archives were moved to another external server due to disk space limitations. In this case, you would modify the hostname and path, and probably the username and password for the catalog entry. Another scenario is that you want to restore archives but not to the Guardium® system that initiated the archive. In this case, you need to add the entries to the catalog on the target restore Guardium system; and delete them from their original catalog. Delete all archive files that you no longer need, for any reason, from the catalog.

An alternative method of moving catalog entries from one set to another is to [Export catalog entries](#) on the Guardium system where the archive files were taken, then [Import catalog entries](#) on the target restore server. In this scenario, you do not need to remove the entries, they are removed when you export them.

### Procedure

1. Click **Manage > Data Management > Catalog Archive**.
2. To add a catalog entry:
  - a. Click **Add**.  
The Add Location pane opens.
  - b. Select an option from the Storage System drop-down.
  - c. Enter a File Name.
  - d. Enter all other details, according to the Storage System you selected. The value for Path depends on the server or protocol type:
    - For SCP - Specify the directory as an absolute path.
    - For SFTP - Specify the directory relative to the SFTP account home directory.
    - For TSM: Specify the directory as an absolute path of the original location.
  - e. Click **Save**.

3. To modify one or more entries:
  - a. Enter a From and To date.
  - b. Optional: Enter a host name or IP of an external server, to filter results for archives stored on that server only.
  - c. Click Search. The page refreshes with the relevant catalog entries.
  - d. Select an entry and modify as relevant.
  - e. Click Save.
4. To remove a catalog entry:
  - a. Enter a From and To date.
  - b. Optional: Enter a host name or IP of an external server, to filter results for archives stored on that server only.
  - c. Click Search. The page refreshes with the relevant catalog entries.
  - d. Select one or more entries and click Remove Selected.
5. Click Done when you are finished.

## Related reference

---

- [Catalog entry APIs](#)
- 

## Data aggregation

Collect and merge information from multiple Guardium® units into a single Guardium Aggregation appliance to offload the reporting and analysis function from the collectors, while also providing a consolidated view of the data from multiple collectors.

### Aggregation Process

---

- Accomplished by exporting data on a daily basis from the collectors to the aggregator (importing daily export files to the aggregator).
- Aggregator then goes over the uploaded files, extracts each file and merges it into the internal repository on the aggregator.

For example, if you are running Guardium in an enterprise deployment, you may have multiple Guardium servers monitoring different environments (different geographic locations or business units, for example). It may be useful to collect all data in a central location to facilitate an enterprise view of database usage. You can accomplish this by exporting data from a number of servers to another server that has been configured (during the initial installation procedures) as an aggregation appliance. In such a deployment, you typically run all reports, assessments, audit processes, and so forth, on the aggregation appliance to achieve a wider view, not always an enterprise view. The Aggregator does not collect data; it presents the data from the collectors.

Aggregation does not summarize or roll-up the data. It merges the records.

See pre-defined aggregation reports at: [Manage > Reports > Data Management > Aggregation/Archive Log and Reports > Guardium Operational Reports > Aggregation/Archive Log - Distributed](#), for example.

By default, all static tables on an aggregator are archived daily. Adding the static tables to the normal purge process eliminates the existence of orphans, freeing up disk space and improving report performance.

Archive and export of static tables on an aggregator includes full static data only on the first day of the month (archive) or when the export configuration changes (export). Use the CLI commands **store archive\_table\_by\_date [enable | disable]** or **show archive\_table\_by\_date**. Other relevant CLI commands are **store aggregator clean orphans** or **show aggregator clean orphans**.

## Hierarchical Aggregation

---

Guardium supports hierarchical aggregation, where multiple aggregators merge upwards to a higher-level, central aggregator. This is useful for multi-level views. For example, you may need to deploy one aggregator for North America aggregating multiple units, and another aggregator for Asia aggregating multiple units, and a central, global aggregator merging the contents of the North America and Asia aggregators into a single corporate view. To consolidate data, all aggregators export data to the global aggregator on a scheduled basis. The global aggregator combines that data into a single database (in the global aggregator), so that reports run on the global aggregator use the consolidated data from all of the lower level aggregators.

## Aggregating, Archiving, and Purging Operations

---

The data is transferred through daily batch files by using SCP. A daily data export is scheduled on the source and a corresponding data import is scheduled on the aggregator. There is an option to use a secondary aggregator in case the primary aggregator is unreachable. On either or both units, archive and purge operations are scheduled to back up and purge data on a regular basis (both to free up space and to speed up access operations on the internal database).

CAS data is also aggregated and archived.

**Important:** When setting the schedule of import on an aggregator, set it to run after export is completed on all collectors.

**Note:** The alert for no traffic is inactive for aggregator servers.

## Orphan cleanup on aggregators

---

When the aggregator includes restored data, orphans cleanup related to the restored data are set to run according to the expiration date set when data was first restored.

If any changes are done through API commands related to the expiration date, this does not affect the date restored data that is available for Orphans cleanup.

For example: The user restores data and wants to keep this data for 7 days. This means the expiration date of this data is 7 days from today and this data is available for orphan cleanup after 7 days.

If the expiration date is changed, for example, set to keep the data for shorter/longer period - it does not affect the date this data is available for orphan cleanup. Pay attention for this especially if you change the expiration period to be longer - in order not to lose data. The rest of the data on the managed unit is available for orphan cleanup as first designed.

## Calculating maximum number of Collectors per Aggregator

---

When a Guardium system is built from an .ISO, a default value of 10 for the maximum number of collectors per aggregator is set.

When a customer upgrades the Guardium system, the system calculates the maximum number of collectors using the following logic:

1. Get number of collectors according to data in internal Guardium table. The default value is 10.
2. If results of step 1 is 0 (no collectors are found), the system sets this value to 10.
3. If a different number of collectors is found, the system will add 20 percent more to the number determined in step 2.
4. For example, if Step 1 did not find any collectors, then Step 2 will set a value of 10, and then Step 3 will add 20% to it and will make it 12.
5. Another example, in Step 1 the system found five collectors exporting to an aggregator. In this case, the value is set to 5. Step 2 is not relevant as result was 5 and not 0. Step 3 will add 20% to 5 and will set this value to 6.

- **[Exporting data](#)**

Export compresses the data of the one day, midnight to midnight, into an encrypted file and sends it from a Guardium collector to a Guardium aggregator, daily. The aggregator has its own schedule to import the encrypted export file. Archive and purge operations can be scheduled on both collectors and aggregators to speed up access operations on the internal database. Purge also frees up space.

- **[Importing data](#)**

After data files are exported from the collector, they reside in a special location on the aggregator until the aggregator appliance executes an import operation to decrypt and merge all data to its own internal database. The Data Import process is scheduled only on an aggregator, or a central manager in a smaller system.

## Related concepts

---

- [Aggregator CLI commands](#)
- 

## Exporting data

---

Export compresses the data of the one day, midnight to midnight, into an encrypted file and sends it from a Guardium® collector to a Guardium aggregator, daily. The aggregator has its own schedule to import the encrypted export file. Archive and purge operations can be scheduled on both collectors and aggregators to speed up access operations on the internal database. Purge also frees up space.

## Before you begin

---

The collector that sends the data and the aggregator to which it is sending data must have the identical System Shared Secret. If not, the export operation works, but the aggregator that receives the data is not able to decrypt the exported file and the import fails. For more information, see [About System Shared Secret](#).

## About this task

---

You can define one export configuration for each Guardium system.

To stop a scheduled export, clear the Export checkbox. You cannot stop an export after clicking Run once now.

## Procedure

---

1. Go to [Manage > Data Management > Data Export](#)
2. Check Export.
3. Specify the data to be exported:
  - Export data older than (required): specify a starting day for the export operation as a number of days, weeks, or months before the current day, which is day zero. Time is measured in calendar days. For example, if today is 24 April, all data that was captured on 23 April is one day old. To archive data yesterday's data and data older than yesterday, specify 1 Day.
  - Ignore data older than: specifies how many days of data are archived. Guardium recommends always specifying Ignore data older than. Ignore data older than must always be greater than Export data older than. When left blank, you export data for all days previous to the date specified by Export data older than. The result is exporting the exact same days of data over and over again, overloading the network and the aggregator with redundant data.  
For example, to export daily data only: Export data older than=1 Day, and Ignore data older than=2 Day
4. The Export Values box is checked by default, meaning all fields that contain sensitive fields are included in the exported data. Clear this option to mask all sensitive fields in the exported data, and replace the fields with **Value~Removed**.
5. In the Host box, enter the IP address or DNS hostname of the aggregator to which this system's encrypted data files are sent. You can optionally specify a second aggregator to export data to more than one aggregator. If you specify two aggregators, Guardium exports to both of them.
6. Click Save to save the export configuration for this unit.
7. Use Scheduling to define a schedule for running this operation.
8. Click Apply: the system attempts to verify that the specified aggregator host accepts data from this unit. If the operation fails, the configuration is not saved, and system responds: A test data file could not be sent to this host. Please confirm the hostname or IP address is entered correctly and the host is online.
9. Optional: Click Run Once Now to run the operation one time.

## What to do next

---

Verify that the export operation succeeded. Go to [Manage > Reports > Data Management > Aggregation/Archive Log](#). Each archive operation shows multiple activities. Check that the status of each activity is Succeeded.

## Related concepts

---

- [Viewing days whose data was not archived or exported](#)

## Importing data

After data files are exported from the collector, they reside in a special location on the aggregator until the aggregator appliance executes an import operation to decrypt and merge all data to its own internal database. The Data Import process is scheduled only on an aggregator, or a central manager in a smaller system.

### Before you begin

The collector that sends the data and the aggregator to which it is sending data must have the identical System Shared Secret. If not, the aggregator that receives the data cannot decrypt the exported file and the import fails. For more information, see [About System Shared Secret](#).

### About this task

Import has no default schedule. Schedule it to start after export is complete. To avoid the possibility of importing files that have not completely arrived, the aggregator does not import files that have changed in the last two minutes. You can define one import configuration for each Guardium unit. Purge can be configured on either the Archive or Export GUI pages.

Do not run more than once a day unless you have a good reason for doing so. For example, data from one or more collectors arrived after an import run. In this case, click Run Once Now to import the additional data.

To stop a scheduled import, clear the Import data checkbox. You cannot stop an import after clicking Run once now.

### Procedure

1. Go to [Manage > Data Management > Import](#)
2. Define the import frequency, by day or by month.
3. Define the Repeat schedule

## Purging data

Data that has been successfully archived should be purged from the Guardium appliance to maintain the disk space. Configure and schedule the purge mechanism during the implementation stage to run nightly: to purge data that is older than a specified number of days.

- [Configuring data purge](#)  
Configure purge in one or both of the Data Archive page or the Data Export page. Although the purge configuration is on the same page, purge is enabled independently of Archive and Export.
- [Purging data to resolve a full disk when the GUI is down](#)  
Learn how to identify a full disk, and what to do about it.

## Configuring data purge

Configure purge in one or both of the Data Archive page or the Data Export page. Although the purge configuration is on the same page, purge is enabled independently of Archive and Export.

### About this task

Important: The Purge configuration is used by both Data Archive and Data Export. The Purge that is configured in the Data Archive page applies to archived data, and in the Data Export page to exported data.

The amount of data that can be stored on the appliance depends on many criteria, including appliance type, disk space, and policy. The data storage period must be adjusted to reflect the optimal balance between data accessibility and quick response time of the system process. Data purge configuration depends on the application and is highly variable, depending on business and auditing requirements.

- The default value for purge is 60 days.
- The purge schedule is not affected during an upgrade.
- To purge many records (10 million or higher), a large batch size setting (500k to 1 million) is the most effective. Using a smaller batch size or NULL results in a much slower purge time for large purges. Smaller purges finish quickly. Specify a large batch size for large purges only. Set the purge size with the GuardAPI [set\\_purge\\_batch\\_size](#).
- When a unit type is changed from managed unit to standalone or vice versa, the default purge schedule is applied.
- Purge does not delete records that are still "in use" (for example: open sessions).

Schedule purge on collectors, after the export or archive. Schedule purge on aggregators after the import.

Important: If purging is activated, and Allow purge without exporting or archiving checkbox is selected, and both Data export and Data Archive are run on the same day, then the first operation that runs probably purges any old data before the second operation's execution. When Data export and Data Archive are both configured, the purge age must be greater than the export age and the archive age. For example, data that is older than one day and younger than two days is archived; data that is older than seven days and younger than eight days is purged.

CAUTION:

There is no warning when you purge data that is not archived or exported by a previous operation.

The purge operation does not purge restored data whose age is within the Don't purge restored data for at least timeframe that is specified by a restore operation.

### Procedure

1. Check the Purge checkbox.
2. Use the Purge data older than field to specify a starting day for the purge operation as a number of days, weeks, or months before the current day, which is day zero. All data from the specified day and all older days is purged, except as noted. The starting purge date must be greater than the Export data older than and Archive data older than values, if export or archive are configured.
3. If the data is exported to a non-Guardium system, check Allow purge without exporting or archiving.
4. Clear Allow purge without exporting or archiving to prevent purge from running before both export and archive are completed. If archive and export are both configured and this checkbox is selected, the purge process runs with the overall process, meaning it runs after the first of export or archive that completes its run. For example, archive is scheduled to run at 01:00 and export is scheduled to run at 03:00. Purge runs immediately after archive, and probably before the export, and therefore there won't be a file to export. If this checkbox is cleared, then purge runs after both archive and export are complete.

## What to do next

Verify that the operation completed successfully. Go to Manage > Reports > Data Management > Aggregation/Archive Log. Each archive operation shows multiple activities. Check that the status of each activity is Succeeded.

## Related concepts

- [Viewing days whose data was not archived or exported](#)

## Purging data to resolve a full disk when the GUI is down

Learn how to identify a full disk, and what to do about it.

## About this task

Two areas can get full on a Guardium appliance which can then cause the GUI to stop:

- The internal database
- The filesystem itself (usually the /var partition)

One or both can become full. Usually it is the database that fills up, which then causes the filesystem to fill up, since the database files are held in the /var partition. If either gets to 90% full, the system automatically stops services, including the GUI.

Auto stop services: By default the appliance stops services including GUI and sniffer when the database or the filesystem reaches 90% full. An internal 'nanny' process checks the status every 5 minutes and takes actions. You can check the current setting in the CLI:

```
xxx.xxx.xxx.com> show auto_stop_services_when_full
```

See [Configuration and control CLI commands](#)

Important notes for auto stop services:

- If the auto\_stop\_services\_when\_full is switched **off**, the system might be filled to 100% preventing all access to the system
- Never set the auto\_stop\_services\_when\_full to **off** unless used temporarily in the specific circumstance described in the answer section
- You must **stop inspection-core** before setting auto\_stop\_services\_when\_full to **off**. This prevents the system filling any further.
- If you attempt to restart stopped services before the space issue is resolved, then the services stop again after 5 minutes. The filesystem and database usage keep increasing in that time. Command to restart stopped services:

```
restart stopped_services
```

Warning: Do not use this command until you are sure that space has been recovered.

### Diagnosing the problem

Internal database: As user cli, check whether the internal database is full with this command:

```
support show db-status used %
```

If the result is 90% or more the GUI should be stopped automatically by auto stop services. It is possible for the database to show over 100% used. It happens when the database files consume more than the set size defined on the system (50% of disk space for collectors, 75% for aggregators). This can happen if system services are not stopped when database reaches 90% or they are restarted manually.

Internal filesystem: To check if /var partition (filesystem) is 90% full or more, run a must gather from cli:

```
support must_gather system_db_info
```

Use fileserver to check the **df -k** output within the **system\_output.txt** file that can be seen in fileserver: **must\_gather/system\_logs/system\_output.txt**, or extracted from the **system.<datetime>.tgz** file once you have downloaded it

Inside the **system\_output.txt** file you can find the detail. In this example the /var is only 65% full:

```
=====2016-11-30 08:36:09 ... Output of df command=====
Filesystem 1024-blocks Used Available Capacity Mounted on
/dev/sda3 10154020 2272668 7357232 24% /
/dev/sda2 28571320 17384504 9712052 65% /var
/dev/sd1 505604 33476 446024 7% /boot
tmpfs 6169768 0 6169768 0% /dev/shm
```

Before the database or the filesystem fills to the "auto stop" level you should receive warnings in the system log (messages file). You can run a **must\_gather** command and look inside the compressed file that gets created to check the latest messages file within

```
support must_gather system_db_info
```

Sample message filesystem space problem errors.

In this example the messages file shows the filesystem is full (DB space may also be full)

```
Nov 23 12:00:13 xxx nanny:[2986]: Nanny is awake.
Nov 23 12:00:13 xxx nanny:[2986]: DB parameters - status 2 db warn level 75 db critical level 90 db auto stop 1.
Nov 23 12:00:13 xxx nanny:[2986]: It is in critical ..Used space on your system is almost full(currently at 93%). Please use
CLI command 'show filesystem usage' to see which directories take too much space to target your clean up.
Nov 23 12:00:13 xxx nanny:[2986]: Email has been sent to admin (admin@admin.com) on the out-of-space issue.
Nov 23 12:00:13 xxx nanny:[2986]: Stopping Guardium Services until used space on your system has been cleaned up.
```

This example shows both the DB and the filesystem (/var partition) NEARLY full (before the auto stop of services)

```
Nov 23 14:13:12 xxx nanny:[10070]: TURBINE DB is configured after nap
Nov 23 14:13:12 xxx nanny:[10070]: Nanny is awake.
Nov 23 14:13:12 xxx nanny:[10070]: DB parameters - status 1 db warn level 75 db critical level 90 db auto stop 1.
Nov 23 14:13:12 xxx nanny:[10070]: Used space on your system is filling up (currently at 88%). Please use CLI command 'show
filesystem usage' to see which directories take too much space to target your clean up.
Nov 23 14:13:12 xxx nanny:[10070]: Email has been sent to admin (admin@admin.com) on the out-of-space issue.
Nov 23 14:13:12 xxx nanny:[10070]: A partition is rapidly filling up. Partition /dev/sda2 (/var) on xxx is on 88 percent usage.
Doing preventive cleaning.
Nov 23 14:13:13 xxx root: 64 bit big mem 24554360 limit is 12277180
Nov 23 14:13:13 xxx nanny:[15110]: Hunting version 35, every 300, for more than 12277180 kb.
Nov 23 14:13:13 xxx nanny:[15110]: Also checking tomcat.
Nov 23 14:13:13 xxx nanny:[15110]: Nanny set memory limit to 12277180
Nov 23 14:13:13 xxx nanny:[15110]: TURBINE DB Already configured before nap
Nov 23 14:13:13 xxx nanny:[15110]: Going for my initial nap.
```

## Procedure

1. If the database is 90% or more full but the filesystem is not 90% full yet:

If the auto stop has been triggered then this stops services such as the GUI, which stops you from making an emergency purge of data via the "Run Once Now" purge option. However, purge from the GUI is still the best way to reduce data in emergency, provided these steps and considerations are followed.

- a. Make sure that the inspection-core is switched **off** on collectors to stop more data flooding into the appliance. Check that NO database commands are running except the show process list. If needed let any running commands finish before the next step.

```
stop inspection-core
xxx.xxx.xxx.com> support show db-processlist running

Id	User	Host	db	Command	Time	State	Info
141791	enchantedg	localhost	TURBINE	Query	0	init	show processlist

Total of running processes: 1
Total of sleep processes: 44
```

- b. Run **restart gui** to gain access to the GUI to perform the once now purge.

- Before starting purge ensure that both Archive and Export are **not selected**, so the system does not first create archive or export files.
- If there is a problem where the GUI keeps going down every five minutes, then consider switching the **auto\_stop\_services\_when\_full** to **off**, only **temporarily**, to allow you to restart the GUI and purge some data. By restarting the GUI on its own, it might only stay running for 5 minutes, and the nanny process might stop the services again before enough data is purged or before you have had time to start the purge.
- If the **auto\_stop\_services\_when\_full** is switched off, the appliance might go on to fill the system to 100%, preventing you from accessing the system at all. Never set the **auto\_stop\_services\_when\_full** to OFF unless you are using it temporarily in the specific circumstance described here. As soon as you have resolved the the space problem, switch it back to ON.

- c. Keep checking the DB full percentage and the Aggregation Archive log to know when the purge process is finished.

- d. When the purge is finished, set the **auto\_stop\_services\_when\_full** back on and then restart the stopped services.

```
store auto_stop_services_when_full on
restart stopped_services
```

- e. Data should start to be collected again. Monitor the system carefully.

- f. Investigate the root cause to ensure the problem does not recur.

- Purging the data does not resolve any root cause of a full database. Check the policy configuration or level of incoming traffic from S-TAPs.

2. If the database size is fine but the filesystem (/var) is full then some system files might be left on the appliance for example:

- If daily exports or archives are failing a temporary file might be left in the system for each day.
- Some old large patch files might be left in the /var/log/guard/patches directory.
- Tomcat service running on the system might be crashing and creating dump files.

The following CLI commands can be used to identify large files.

- - **show filesystem usage**: Shows types of files (database, log, gim) and how much space is used by them. Log files usually can be deleted.
  - **support show large\_files 10 0**: Shows files larger than 10MB older than 0 days. Consider the largest ones for removal first.

You might need to work with IBM Technical Support to carefully check for large files and consider ones for deletion.

3. Use of these two options to delete files.

- support clean log\_files, for example:

```
support clean log_files <file to delete, full path>
```

- diag-> 4) Perform Maintenance Actions -> 3) Clean Disk Space
  - Pick the directory where the large files reside.
  - Carefully enter a filter term to isolate the specific files that will be removed. Work with IBM Support if needed.
  - Check the list that is returned
  - Confirm you want the files to be removed

## Related concepts

- [Configuration and control CLI commands](#)

## Related information

---

- [What can I do if I see my Guardium system getting full?](#)
  - [Why is my Guardium internal database filling up?](#)
  - [How to alert on the Guardium internal database filling up](#)
  - [Database and disk full alerts \(Disk and DB Health analyzer feature\)](#)
- 

## Configuring system backup

System backups store all the necessary data and configuration values to restore a Guardium Server. Configure and schedule regular system backups during the implementation stage.

### About this task

---

A system backup is a full backup of the Guardium database and selected configuration files, such as groups, queries, reports, audit processes, alerts, and policies. In virtualized environments, you can create a backup by making an actual snapshot of the Guardium® system. Use the snapshot to restore a failed system. In this case, it is not necessary to keep more than three rolling copies. It is important to back up the aggregators. A weekly backup is recommended, especially for the central manager. However, some users might opt for a slightly longer cycle. Tip: In a managed environment with aggregation, you might choose not to back up managed collectors. Always back up stand-alone collectors.

Suggested data retention for disaster recovery

- Keep a rolling three months full backup from each unit (minimum one month).
- Keep a rolling 2-weeks worth of daily archives from the managed collectors.
- Full or system backups
  - Weekly or daily full backups of the central manager unit (assuming a stand-alone central manager).
  - Monthly for aggregators and collectors during a quiet off-hour period.

Data and configuration values are stored in separate encrypted files and sent to the specified destination by using the transfer method that is configured for backups on the system. For more information about the encryption used for backup files, see the [File backup cipher](#) section of [Cipher suites](#)

Note: You cannot make new buckets nor delete any buckets from the Guardium UI/CLI.

Note: During a file transfer, if the backup file transfer fails, the last file in each set of backup or archive files (for example, backup, configuration backup, archive, CSV archive) is saved in the diag/current folder. When the backup file destination is again online, you can manually transfer the backup files from the diag/current folder to the destination. The set of backup or archive files is saved in the diag/current folder only if the file transfer fails. If a file transfer fails during another backup file transfer, the set of backup or archive files is saved in the diag/current folder. However, to avoid saving too many files and running out of disk space, only the latest file of each type are saved. The earlier backup files are overwritten.

To prevent backup scripts from filling up /var:

- Before it starts, the backup process checks for room in /var. This process also warns the user if the space is insufficient for backup.
- The archive process checks the size of the static tables and verifies that /var has space to create the archive.
- An error is logged in the log file and GUI if the backup is over 50%. For example:

```
ERROR: /var backup space is at 60% used. Insufficient disk space for backup.
```

## Procedure

---

1. Go to [Manage > Data Management > System Backup](#).
2. Select a storage method and enter the configuration details. Depending on how the Guardium system is configured, only some of the options are available. For more information about configuring the archive and backup storage methods, see [Configuring external storage](#), and [store storage-system](#) and [show storage-system](#) commands ([store storage-system](#)).
3. Select one or both of the backup options:
  - Configuration: to back up important definitions.
  - Data: to back up all data. (Not needed if you are archiving data regularly.)
4. Use the Scheduling section to define a schedule for backup.
5. Click Save to verify and save the configuration changes. The system attempts to verify the configuration by sending a test data file to that location. If the operation fails, an error message displays and the configuration is not saved.
6. Optional: Click Run Once Now to run the operation once.

## What to do next

---

Verify that the operation completed successfully. Go to [Manage > Reports > Data Management > Aggregation/Archive Log](#). Each backup operation shows multiple activities. Check that the status of each activity is Succeeded.

## Restoring a Guardium system

Each type of guardium system (collectors, aggregators, and central manager) have different purposes and store data in different ways. Use the appropriate recovery strategies for each system type. The recovery strategy that is used also depends on whether the system that must be recovered is a stand-alone appliance or is used with other systems.

- [Before you restore your Guardium system](#)  
Review the prerequisites to restoring, and understand the restore flow.

- [Restoring a standalone collector](#)  
Follow these steps to restore a standalone collector.
- [Restoring a collector with an aggregator that is not centrally managed](#)  
Follow these steps to restore a collector associated with an aggregator, but not in a centralized environment.
- [Restoring an aggregator that is not centrally managed](#)  
Follow these steps to restore an aggregator that is not centrally managed.
- [Restoring a centrally managed collector](#)  
Follow these steps to restore a centrally managed collector.
- [Restoring a centrally managed aggregator](#)  
Restore a centrally managed aggregator.
- [Restoring a dedicated central manager \(no data aggregation\)](#)  
Take the following steps to restore a dedicated central manager that does not aggregate data.
- [Restoring default and custom certificates](#)  
12.1 and later Backup and restore process restores only certificates that are not expired rather than restoring all certificates.

## Before you restore your Guardium system

Review the prerequisites to restoring, and understand the restore flow.

### Before you begin

Before you start the appliance recovery process, verify that you have the following information:

- New physical or virtual appliance.
- ISO image of Guardium software.
- The same patches that were installed on the appliance when the last system backup was taken.
- Latest system backup files.
- Daily archive files.
- License, SSL certificates, and any settings that must be set manually.

For information about what data is restored during a backup restore, see [restore backup](#).

### About this task

The following items are not backed up and must be installed or configured manually to complete the disaster recovery process:

- License - Reinstall the license manually.
- SSL Certificate: SSL certificates are not backed up. You need to reinstall them manually.
- Language: Use the CLI command [store language](#) to change from English (default).
- Network Time Protocol (NTP) settings: Use the CLI commands [store system time server](#) with the **hostnames** and **state** options to complete NTP server configuration.
- Time zone: Use the CLI command [store system clock timezone](#) to configure the system time zone.
- Enterprise search data: Data is not saved in the backup, and is not available in dashboards on a restored system.
- If you are using Tivoli Storage Manager or Centera as a storage location, configure the appliance to support it before you attempt to restore the backup files.

**Tip:** If you restore a configuration system backup from an appliance where SAML was configured, and then restore the system on a different appliance with different hostname or IP address, you must reconfigure SAML on the new appliance after you restore. Most identity providers (IdPs) require each hostname or IP to have its own registration. Therefore, the original registration of the appliance where the backup was taken is not valid on the second appliance where it is restored.

**Note:** As part of the **restore backup** dialog, you can choose to either override or restore configuration details for risk spotter and for central manager and managed units registration, as follows.

- Enter Y to maintain the current configuration of the central manager and managed units in your Guardium system.
- Enter N to restore the managed configuration of your Guardium environment from your system back up.

**Limitation:** Restored data does not include quick search data.

### Procedure

To start the restore, enter the CLI command [restore backup](#).

The script has a few options, depending on what you want to do. The following example shows many of the options, but your system might differ.

```
restore backup

This procedure will restore a DATA or CONFIG backup file or both onto a v11.0 system.

Continue (y/n)?
y
List of available DATA backup files:

1. 2020-02-12-0402-<server>-SQLGUARD_DATA-11.0.tgz

Please choose a DATA file to restore (1-1, i to import, s to skip, or q to quit):
Please choose i to import, s to skip, or q to quit):
i

List of available file transfer methods:

1. SCP
2. FTP
```

```

3. TSM
4. CENTERA
5. AMAZONS3
6. IBMCloud
7. SFTP
8. IBMCOS

Please enter the number of your choice: (q to quit) 1
Enter the remote host: <remote host>
Enter the remote host username: <username>
Enter the remote directory: <remote dir>
Enter the remote file name (file name may use wildcard *): 2020-02-12-0402-<server>-11.0.tgz
Enter the password for <username>@<remote host>? *****

Enter the SCP port if you need to use a special port.
Enter "0" or press "Enter key" to use the default port.

Attempting to retrieve file. It may take time. Please wait.
During the transfer, please do not enter the password or answer any questions.
spawn /usr/bin/scp -4 <remote host user name>@<remote host>:<remote directory>2020-02-12-0402-<server>-SQLGUARD_CONFIG-11.0.tgz
/var/tmp/import_file_transfer.VEakM/tmp/
Warning: Permanently added '<remote host>' (RSA) to the list of known hosts.
CentOS release 5.3 (Final)
WARNING !!

This computer system including all related equipment, network devices
(specifically including Internet access), are provided only for authorized
use. Unauthorized use may subject you to criminal prosecution. By accessing
this system, you have agreed to the term and condition of use and your
actions will be monitored and recorded.
echo `uname -a`
<username>@<remote host>'s password:
2020-02-12-0402-<server>-11.0.tgz 100% 5659KB 42.9MB/s 00:00
SUCCESS: 2020-02-12-0402-<server>-11.0.tgz transferred to /var/dump/restore

List of available CONFIG backup files:

1. 2020-02-12-0402-<server>-SQLGUARD_CONFIG-11.0.tgz
2. 2020-02-12-0403-<server>-SQLGUARD_CONFIG-11.0.tgz
3. 2020-02-12-0403-<server>-SQLGUARD_CONFIG-11.0.tgz.dec

Please choose a CONFIG file to restore (1-3, i to import, s to skip, or q to quit):
1

Decrypting the CONFIG file...
Extracting the CONFIG file...

CONFIG backup file attributes (to be restore):

Name: 2020-02-12-0402-<server>-11.0.tgz
Type: Manager/Aggregator
Version: 11.0
GPU: 0
CFP: 0
Bundle: 0
Snif: 0

```

## Related concepts

---

- [File handling CLI commands](#)

## Restoring a standalone collector

---

Follow these steps to restore a standalone collector.

### Procedure

---

1. Use an ISO that is appropriate for your appliance.  
For example, to restore a collector, use a collector ISO; for an aggregator, use an aggregator ISO.
2. Apply the license.
3. Make sure that your newly built appliance is at an equal or later version than the source appliance from which the backup was taken. If the appliance is at an earlier version, then apply the required GPU, bundle, and sniffer patches to bring the appliance to the same patch level as it was when the last backup was taken.  
For example, if the source appliance is a version 11.4 Guardium system that was patched with bundle 11.0p450 and sniffer patch 11.0p4020 and the new appliance was built from ISO 11.3, choose one of the following options:
  - Install 11.4 GPU. Then, apply appliance bundle version 11.0p450 or later and sniffer patch version 11.0p4020 or later.  
Or,
  - Install GPU version 11.5 or later.
4. Use the [restore backup](#) CLI command to restore the data and configuration backups.  
For more information, see [Before you restore your Guardium system](#).
5. If needed, restore the archive files for any missing days.

## Related concepts

---

- [File handling CLI commands](#)

## Restoring a collector with an aggregator that is not centrally managed

Follow these steps to restore a collector associated with an aggregator, but not in a centralized environment.

### Procedure

1. Use an ISO that is appropriate for your appliance.  
For example, to restore a collector, use a collector ISO; for an aggregator, use an aggregator ISO.
2. Apply the license.
3. Make sure that your newly built appliance is at an equal or later version than the source appliance from which the backup was taken. If the appliance is at an earlier version, then apply the required GPU, bundle, and sniffer patches to bring the appliance to the same patch level as it was when the last backup was taken.  
For example, if the source appliance is a version 11.4 Guardium system that was patched with bundle 11.0p450 and sniffer patch 11.0p4020 and the new appliance was built from ISO 11.3, choose one of the following options:
  - Install 11.4 GPU. Then, apply appliance bundle version 11.0p450 or later and sniffer patch version 11.0p4020 or later.
  - Or,
  - Install GPU version 11.5 or later.
4. Use the [restore backup](#) CLI command to restore the data and configuration backups.  
For more information, see [Before you restore your Guardium system](#).
5. Restoring the archive files is optional because the data already exists on an aggregator.

### Related concepts

- [File handling CLI commands](#)

## Restoring an aggregator that is not centrally managed

Follow these steps to restore an aggregator that is not centrally managed.

### About this task

Alternatively, to restore data backup, consider aggregating data again from collectors, depending on the number of collectors and the retention period requirements on the collectors and aggregator.

### Procedure

1. Use an ISO that is appropriate for your appliance.  
For example, to restore a collector, use a collector ISO; for an aggregator, use an aggregator ISO.
2. Apply the license.
3. Make sure that your newly built appliance is at an equal or later version than the source appliance from which the backup was taken. If the appliance is at an earlier version, then apply the required GPU, bundle, and sniffer patches to bring the appliance to the same patch level as it was when the last backup was taken.  
For example, if the source appliance is a version 11.4 Guardium system that was patched with bundle 11.0p450 and sniffer patch 11.0p4020 and the new appliance was built from ISO 11.3, choose one of the following options:
  - Install 11.4 GPU. Then, apply appliance bundle version 11.0p450 or later and sniffer patch version 11.0p4020 or later.
  - Or,
  - Install GPU version 11.5 or later.
4. Use the [restore backup](#) CLI command to restore the data and configuration backups.  
For more information, see [Before you restore your Guardium system](#).
5. If needed, restore the archive files for any missing days.

### What to do next

When restoring data from an aggregator to a new system with a different hostname, the new system shows collectors from the source aggregator, and the collectors on the new system. After completing the restore:

1. On each of the old collectors define a data export to the new aggregator and click Save.
2. Clear the Export checkbox in the data export (that you just defined) and click Save.

### Related concepts

- [File handling CLI commands](#)

## Restoring a centrally managed collector

Follow these steps to restore a centrally managed collector.

## About this task

---

A centrally managed collector stores its configuration data on the central manager; restore data is not required.

## Procedure

---

1. Use an ISO that is appropriate for your appliance.  
For example, to restore a collector, use a collector ISO; for an aggregator, use an aggregator ISO.
2. Register the newly built collector with central manager (licenses are pooled from central manager).
3. Make sure that your newly built appliance is at an equal or later version than the source appliance from which the backup was taken. If the appliance is at an earlier version, then apply the required GPU, bundle, and sniffer patches to bring the appliance to the same patch level as it was when the last backup was taken.  
For example, if the source appliance is a version 11.4 Guardium system that was patched with bundle 11.0p450 and sniffer patch 11.0p4020 and the new appliance was built from ISO 11.3, choose one of the following options:
  - Install 11.4 GPU. Then, apply appliance bundle version 11.0p450 or later and sniffer patch version 11.0p4020 or later.  
Or,
  - Install GPU version 11.5 or later.
4. Use the [restore backup](#) CLI command to restore the data backup.  
This step might be optional if the environment includes an aggregator and data from the collector also exists on the aggregator. (You do not need to restore the configuration backup because the definitions are pooled from the central manager.)  
For more information, see [Before you restore your Guardium system](#).
5. Use the [store system shared secret](#) CLI command to set the shared secret to enable communication with central manager. The shared secret encrypts communication of the appliance with central manager.
6. Optional: Restore archive files for missing days, as needed. This step is not required if you are not restoring data backup.

## Related concepts

---

- [File handling CLI commands](#)

## Restoring a centrally managed aggregator

---

Restore a centrally managed aggregator.

## About this task

---

The configuration data of a centrally managed aggregator is stored on the central manager. It is not necessary to restore the data on the aggregator during disaster recovery.

## Procedure

---

1. Use the appropriate ISO image to build an appliance.
2. The newly built appliance must be of an equal or higher version than the source appliance from which the backup was taken. If the version is lower, apply the required GPU, bundle, and sniffer patches to bring the appliance to the same patch level as it was when the last backup was taken.  
As an example, if the source appliance is a version 11.4 Guardium system that was patched with bundle 11.0p450 and sniffer patch 11.0p4020 and the new appliance was built from ISO 11.3, choose one of the following options:
  - Install 11.4 GPU. Then, apply appliance bundle version 11.0p450 or up and sniffer patch version 11.0p4020 or up.
  - Install GPU version 11.5 or up.
3. Enable all required network settings.
4. If the source appliance was a managed unit, you must register your newly built appliance with the central manager (licenses are pooled from central manager).
5. Shared secret must be set to enable communication with central manager. Shared secret is used to encrypt communication of the appliance with central manager.  
Use CLI command store system shared secret to complete this step.
6. Restore the data backup. It is not necessary to restore the configuration backup because the definitions are pooled from central manager.
7. Restore archive files for missing days, as needed.

## What to do next

---

When you restore data from an aggregator to a new system with a different hostname, the new system shows collectors from the source aggregator, and the collectors on the new system. After completing the restore:

1. On each of the old collectors, define a data export to the new aggregator and Save.
2. Clear the Export checkbox in the data export (that you just defined) and Save.

## Related concepts

---

- [File handling CLI commands](#)

## Restoring a dedicated central manager (no data aggregation)

---

Take the following steps to restore a dedicated central manager that does not aggregate data.

## About this task

When you restore a unit from the backup taken from the different environment that contains appliances that are not registered to the new restored system, go to the Managed Unit Groups page in the new environment and modify the groups accordingly. If there are distributed reports based on these groups, they are corrected automatically when you save the changes in the Managed Unit groups page.

## Procedure

1. Use an ISO that is appropriate for your appliance.  
For example, to restore a collector, use a collector ISO; for an aggregator, use an aggregator ISO.
2. Apply the license.
3. Make sure that your newly built appliance is at an equal or later version than the source appliance from which the backup was taken. If the appliance is at an earlier version, then apply the required GPU, bundle, and sniffer patches to bring the appliance to the same patch level as it was when the last backup was taken.  
For example, if the source appliance is a version 11.4 Guardium system that was patched with bundle 11.0p450 and sniffer patch 11.0p4020 and the new appliance was built from ISO 11.3, choose one of the following options:
  - Install 11.4 GPU. Then, apply appliance bundle version 11.0p450 or later and sniffer patch version 11.0p4020 or later.
  - Or,
  - Install GPU version 11.5 or later.
4. Use the [restore backup](#) CLI command to restore the configuration backup.  
For more information, see [Before you restore your Guardium system](#).

## Related concepts

- [File handling CLI commands](#)

## Restoring default and custom certificates

12.1 and later Backup and restore process restores only certificates that are not expired rather than restoring all certificates.

During config system backup, certificates are automatically backed up.

For custom certificates, restore it from the backup file always.

For default certificates, check the expiration date of the certificate in the backup file and the current target system. If the certificate in the backup file is newer than the current certificate on the system, restore it. If the certificate in the backup file is earlier than the current certificate on the system, don't restore it.

The following table lists the scenarios to show the behavior for default and custom certificates when they are backed up from the source version and restored to the target version.

Table 1. Scenarios for restoring default and custom certificates

| Type of certificate                                                         | Source version                      | Target version                                                                                                             | Restore process                                                         |
|-----------------------------------------------------------------------------|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Default certificate, custom certificate, or default and custom certificates | Certificate is expired.             | Certificate is expired or not expired.                                                                                     | No changes in target.                                                   |
| Default certificates                                                        | Certificate is not expired.         | The expiration date of a certificate in target is later than the expiration date of the certificate in source.             | No changes in target.                                                   |
|                                                                             | Certificate is not expired.         | The expiration date of certificate in target is earlier than the expiration date of certificate in source.                 | Certificate in target replaces the certificate in source.               |
|                                                                             | Certificate is not expired.         | Certificate is expired.                                                                                                    | Certificate in source replaces the certificate in target.               |
|                                                                             | Certificate is not present.         | Certificate is present.                                                                                                    | No changes in target.                                                   |
|                                                                             | Certificate is not expired.         | Certificate is not present.                                                                                                | Certificate in source is added to the keystore in target.               |
| Custom certificates                                                         | Custom certificate is not expired.  | The expiration date of a custom certificate in target is later than the expiration date of custom certificate in source.   | No changes in target.                                                   |
|                                                                             | Custom certificate is not expired.  | The expiration date of a custom certificate in target is earlier than the expiration date of custom certificate in source. | Custom certificate in target replaces the custom certificate in source. |
|                                                                             | Custom certificate is not expired.  | Custom certificate is expired.                                                                                             | Custom certificate in source replaces the certificate in target.        |
|                                                                             | Custom certificate is not present.  | Custom certificate is present.                                                                                             | No changes in target.                                                   |
|                                                                             | Custom certificate is not expired.  | Custom certificate is not present.                                                                                         | Custom certificate in source is added to the keystore in target.        |
| Default and custom certificates                                             | Custom certificate is not expired.  | Default Guardium certificate is not expired.                                                                               | Custom certificate overwrites default.                                  |
|                                                                             | Default certificate is not expired. | Custom Guardium certificate is expired.                                                                                    | Default Guardium certificate is added to the keystore in target.        |

## Enabling SSH key pairs for data archive, data export, data mart

You can use SSH key pairs for authentication, instead of passwords, for archiving and exporting results, archiving data, and exporting data marts.

## About this task

The Guardium system generates SSH keys specific to the type of transfer (archive, export, data mart), and propagates them to remote hosts that support SCP connections. At the central manager level, you can generate SSH keys across the deployment and propagate them to remote hosts. The remote host gets a copy of the public-transfer-key, and the Guardium appliance retains the private part of the SSH key pair, allowing the data transfer without a password.

The two directories that contain the SSH key details (/opt/IBM/Guardium/etc/ssh/ssh-keys/tomcat/ and /opt/IBM/Guardium/etc/ssh/ssh-keys/transfer/) are backed up into the CONFIG backup file when you run the CLI command **backup system**. When you restore with the CLI command **restore backup**, the files from these two directories are restored into the current appliance. The restore process does not overwrite any existing files in the current appliance that are newer (last modified timestamp).

## Procedure

1. Log in to the Guardium system CLI as admin cli.
2. Enable the feature by entering `store system scp-ssh-key-mode on`
3. Verify that the feature is enabled by entering `show system scp-ssh-key-mode`.  
The response is `scp-ssh-key-mode is enabled`
4. Create the SSH key pair, which can be used for data transfer, by entering  
`store system public-transfer-key create`.  
(Alternatively, use the API command `grdapi generate_transfer_key`.)
5. Verify that the key was made and display the public portion of the key, by entering  
`show system public-transfer-key`
6. Install the public part of the SSH key on the remote host and users account for data transfer, by using one of these methods:
  - Copy the public part of the key and add it into the .ssh/authorized\_keys of the user on the remote host.
  - Run the command `export-public-transfer-key`.

```
...>export-public-transfer-key
This operation will force a new set of ssh keys onto the remote host specified. The keys will be put into the .ssh/author
Continuing ...
Please enter a valid host which will adopt the public transfer-key.
10.12.12.45
Please enter a valid user for the host.
admin
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/opt/IBM/Guardium/etc/ssh/ssh-keys/transfer/id_rsa.pub"
```

  - `grdapi export_transfer_key`
    - On the central manager, copy the unique public-transfer-key of each managed unit to the remote host, by entering:  
`grdapi export_transfer_key host="remote_host_1" user="user1" password="password" api_target_host=all`
    - On a managed unit, copy the specific, unique, public-transfer-key of the managed unit to the remote host, by entering:  
`grdapi export_transfer_key host="remote_host_1" user="user1" password="password"`

The key is imported, and you can run data archive, data export, and system backup to the remote host and user without needing a password.

## What to do next

It is good practice, and required in many environments, to periodically refresh the keys.

1. In the CLI, run the command `system public-transfer-key regenerate` to refresh the keys.
2. Delete the old keys from one or more remote hosts by entering **system public-transfer-key delete**.
3. Import the new keys into the host as described in step 6.

To archive and export results, archive data, and export data marts, see [Transferring data to a remote host by using SSH key pairs for authentication](#).

## Related reference

- [API command: generate\\_transfer\\_key](#)
- [API command: export\\_transfer\\_key](#)

## Transferring data to a remote host by using SSH key pairs for authentication

You can archive and export results, archive data, and export data marts with SSH key pairs for authentication, instead of usernames and passwords.

## Before you begin

Ensure that:

- If you are adding an SSH key pair to a data mart, the data mart is defined.
- The SSH key feature is enabled.
- The SSH key pairs were generated.
- The public part of the key, `public-transfer-key`, was copied to the remote host.

For more information, see [Enabling SSH key pairs for data archive, data export, data mart](#).

## About this task

These grdapi commands have a new parameter, ssh\_keys\_active. When ssh\_keys\_active=1, the system transfers data with the SSH key pairs, instead of a username and password. You can update an existing archive, export, or data mart by using these APIs.

- **grdapi configure\_archive**
- **grdapi datamart\_update\_copy\_file\_info**
- **grdapi datamart\_validate\_copy\_file\_info**
- **grdapi configure\_results\_archive**
- **grdapi configure\_results\_export**

You can also configure a new results archive, results export, and data archive, by using the relevant APIs.

The user and password details that are defined in the Data Archive, Results Archive, and Results Export pages are still valid after you define SSH key pairs. They function as a backup to the SSH key authentication. The UI does not show that you defined SSH key pairs.

## Procedure

---

Run any of the APIs with the parameter ssh\_keys\_active. For example,

- `grdapi configure_archive archiveOlderThan=1 archiveValues=1 destHost="n.n.n.n" ignoreOlderThan=30 protocol="scp" targetDir="/var/tmp" userName="root" ssh_keys_active=1`
- `grdapi datamart_update_copy_file_info destinationHost="n.n.n.n" destinationPath="/var/tmp/" destinationUser="root" transferMethod="SCP" Name="Export:Full SQL" ssh_keys_active=1`
- `grdapi datamart_validate_copy_file_info destinationHost="n.n.n.n" destinationPath="/var/tmp/" destinationUser="root" transferMethod="SCP" ssh_keys_active=1`
- `grdapi configure_results_archive archiveOlderThan=1 archiveValues=1 destHost="n.n.n.n" ignoreOlderThan=30 protocol="scp" targetDir="/var/tmp" userName="root" ssh_keys_active=1`
- `grdapi configure_results_export destHost="n.n.n.n" protocol="scp" targetDir="/var/tmp" userName="root" port=22 ssh_keys_active=1`

## Configuring external storage

---

Archive files can be sent using SCP or FTP protocol, or to a configured external storage system (Amazon S3, EMC Centera, Tivoli Storage Manager, IBM COS, and IBM Cloud). You can define a single archiving configuration for each Guardium® system.

- [Configure an Amazon S3 \(Amazon Simple Storage Service\) target for archive or backup](#)  
Export to Amazon S3 is not enabled by default. After you enable Amazon S3, you can configure it for archives and backup. Learn how to enable the service, and understand the configuration parameters that are used in the archive and backup pages.
- [Configuring an IBM COS \(formerly Cleversafe\) target for archive or backup](#)  
Export to IBM COS is not enabled by default. After you enable IBM COS, you can configure it for archives and backup. Learn how to enable the service, and understand the configuration parameters used in the archive and backup pages.
- [Configure an EMC Centera target for archive or backup](#)  
Export to EMC Centera is not enabled by default. After you enable EMC Centera, you can configure it for archives and backup. Learn how to enable the service, and understand the configuration parameters that are used in the archive and backup pages.
- [Configuring an SCP or SFTP target for archive or backup](#)  
Export by secure copy (SCP) or SFTP (secure file transfer protocol, formerly FTP) are used to archive and backup to the local database server. These options are enabled by default.
- [Configure a Tivoli Storage Manager \(TSM\) archive or backup](#)  
Export to TSM (Tivoli Storage Manager) is not enabled by default. After you enable TSM, you can configure it for backups. Learn how to enable the service, and understand the configuration parameters that are used in the backup page.

## Configure an Amazon S3 (Amazon Simple Storage Service) target for archive or backup

---

Export to Amazon S3 is not enabled by default. After you enable Amazon S3, you can configure it for archives and backup. Learn how to enable the service, and understand the configuration parameters that are used in the archive and backup pages.

### Before you begin

---

- An Amazon account and registration for the S3 service.
- Amazon S3 credentials:
  - Access Key ID: identifies user as the party responsible for service requests. It needs to be included in each request. It is not confidential and does not need to be encrypted. (20-character, alphanumeric sequence).
  - Secret Access Key: The Secret Access Key (40-character sequence) is associated with Access Key ID calculating a digital signature that is included in the request. The Secret Access Key is a secret, for use only by AWS and the user. This key is just a long string of characters (and not a file) that is used to calculate the digital signature that needs to be included in the request. The Secret Access Key is encrypted when saved into the database.
- S3 Bucket Name: Every object that is stored in Amazon S3 is contained in a bucket. Buckets partition the namespace of objects that are stored in Amazon S3. Within a bucket, you can use any names for your objects, but bucket names must be unique across all of Amazon S3.
- The clock time of Guardium system must be correct (within 15 minutes). Otherwise, requests are not accepted. If the Guardium system time is not correct, set the correct time by using the following CLI commands:

```
show system time_server hostnames
store system time_server hostnames (for example, ntp.xxx.yyy.example.com)
store system time_server state on
```

## Procedure

---

1. Enable Amazon S3 archive or backup from the Guardium CLI by entering one or both of these commands:

```
store storage-system amazon_s3 archive on
store storage-system amazon_s3 backup on
```

2. In Manage > Data Management > System Backup or Data Archive pages, select Amazon S3.

3. Enter the Bucket Name.

4. Select the Authentication Type, and its parameters:

- Security Credentials

This is the legacy authentication type. It requires the following parameters:

- Access Key ID
- Secret Access Key

- IAM Role

This authentication type allows the assumption of an *IAM Instance Profile* by specifying the following parameters:

- Access Key ID
- Secret Access Key
- Role ARN

Unlike the legacy *Security Credentials*, *IAM Role* uses temporary credentials to connect to S3. To configure *IAM Role* authentication:

- Create a user in AWS IAM. Make a note of the *Access Key ID* and *Secret Access Key*.
- Create the following policy and associate it with the user:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Action": [
 "iam>ListRoles",
 "sts:AssumeRole"
],
 "Resource": "*"
 }
]
}
```

- Create a new role and set a trust relationship for the user. For example:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Effect": "Allow",
 "Principal": {
 "Service": "ec2.amazonaws.com",
 "AWS": "arn:aws:iam::123456789012:user/guarduser"
 },
 "Action": "sts:AssumeRole"
 }
]
}
```

- Create the following policy and associate it with the role:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "VisualEditor0",
 "Effect": "Allow",
 "Action": [
 "s3:GetObject",
 "s3>ListAllMyBuckets",
 "s3>ListBucket",
 "iamGetInstanceProfile",
 "sts:AssumeRole"
],
 "Resource": "*"
 }
]
}
```

- To authenticate with Guardium, use the *Access Key ID* and *Secret Access Key* of the user and the *Role ARN* of the instance profile role. Find the *Role ARN* by viewing the role in AWS IAM.

- IAM instance Profile

This authentication type only works when using a Guardium instance deployed on AWS EC2. To configure *IAM instance Profile* authentication, create the following AWS policy and associate it with an IAM role:

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "VisualEditor0",
 "Effect": "Allow",
 "Action": [
 "s3:PutObject",
 "s3:GetObject",
 "s3>ListAllMyBuckets",
 "s3>ListBucket",
 "iamGetInstanceProfile",
 "s3:DeleteObject"
],
 "Resource": "*"
 }
]
}
```

```

 "iam>ListInstanceProfilesForRole",
 "sts_ASSUMERole"
],
 "Resource": "*"
}
}

```

Authentication works once the role has been associated with the instance.

Important: For the latest information about AWS security credentials and IAM roles for Amazon EC2, read the Amazon AWS documentation.

- Enter or select values for these definitions use in all types of Amazon S3 backups:

- Region
- Port
- Storage class
- Backup: Configuration or Data

- Optional: Schedule the backup in the lower part of the page. For more details, see [Scheduling](#).

- Click Save.

## Related tasks

---

- [Configure data archive](#)
- [Archiving \(audit\) results](#)
- [Configuring system backup](#)

## Related information

---

- [store storage-system](#)

## Configuring an IBM COS (formerly Cleversafe) target for archive or backup

Export to IBM COS is not enabled by default. After you enable IBM COS, you can configure it for archives and backup. Learn how to enable the service, and understand the configuration parameters used in the archive and backup pages.

## Before you begin

---

Note: Cleversafe is now IBM Cloud Object Storage (COS) on IBM Cloud.

Restriction: External storage on IBM COS is not supported for IPV6.

Prepare these details before you begin:

- Authentication endpoint URL
- IBM COS credentials:
  - Access Key ID: identifies user as the party responsible for service requests. It needs to be included in each request. It is not confidential and does not need to be encrypted. (20-character, alphanumeric sequence).
  - Secret Access Key: The Secret Access Key (40-character sequence) is associated with Access Key ID calculating a digital signature that is included in the request. It is a secret, for use only by IBM COS and the user. This key is just a long string of characters (and not a file) that is used to calculate the digital signature that needs to be included in the request. Secret Access Key is encrypted when saved into the database.
- Bucket Name: Buckets partition the namespace of objects in the storage. Within a bucket, you can use any names for your objects.
- The clock time of Guardium® system must be set to the correct local time. Otherwise, requests are not accepted. If the Guardium system time is not correct, set the correct time by using the following CLI commands:

```

show system time_server hostnames
store system time_server hostnames (for example, ntp.xxx.yyy.example.com)
store system time_server state on

```

## Procedure

---

- Enable IBM COS archive or backup from the Guardium CLI by entering the relevant command:

```

store storage-system IBMCOS archive on
store storage-system IBMCOS backup on

```

- In Manage > Data Management > System Backup or Data Archive pages, select IBM COS (Formerly Cleversafe).
- Enter the Authentication endpoint URL.
- Enter the Access Key ID.
- Enter the Secret Access Key.
- Select the Bucket Name.
- Optional: Schedule the backup in the lower part of the page. For more details, see [Scheduling](#).
- Click Save.
- If you are archiving or backing up by using the HTTPS protocol, you must store the rootca and intermediate certificate, if applicable, into the Tomcat keystore by running the CLI command **store certificate keystore trusted console**. For more information, see [store certificate keystore](#).

## Related tasks

---

- [Configure data archive](#)
- [Archiving \(audit\) results](#)
- [Configuring system backup](#)

## Related information

---

- [store storage-system](#)
  - [Certificate CLI commands](#)
- 

## Configure an EMC Centera target for archive or backup

Export to EMC Centera is not enabled by default. After you enable EMC Centera, you can configure it for archives and backup. Learn how to enable the service, and understand the configuration parameters that are used in the archive and backup pages.

### Before you begin

---

- License with username and password from EMC.
- Establish an account with EMC Centera on the network (requires an IP address and a ClipID)

Note: This procedure also supports Dell EMC ECS 3.5.x for Guardium 11.1 and later.

### Procedure

---

1. Enable Centera storage on Guardium® by entering the CLI command:

```
store storage-system centera backup ON
show storage-system
```

2. In Manage > Data Management > System Backup or Data Archive pages, select EMC Centera.
3. Enter Retention: the number of days to retain the data. The maximum is 24855 (68 years). If you want to save it for longer, you can restore the data later and save it again.
4. Enter Centera Pool Address: the Centera Pool Connection String; for example: 10.2.3.4,10.6.7.8?/var/centera/us1\_profile1\_rwe.pea.txt. This IP address and the .pea file come from EMC Centera. The question mark is required in the path. The .../var/centera/... path name is important as the backup might fail if the path name is not followed. The .pea file gives permissions, username, and password authentication per Centera backup request.
5. Click Upload PEA File to upload a Centera .pea file to be used for the connection string. If the message Cannot open the pool at this address.. appears, check the size of the Guardium system hostname.
6. Optional: Schedule the backup in the lower part of the page. For more details, see [Scheduling](#).
7. Click Save.

### Related tasks

---

- [Configure data archive](#)
- [Archiving \(audit\) results](#)
- [Configuring system backup](#)

### Related information

---

- [store storage-system](#)
- 

## Configuring an SCP or SFTP target for archive or backup

Export by secure copy (SCP) or SFTP (secure file transfer protocol, formerly FTP) are used to archive and backup to the local database server. These options are enabled by default.

### Procedure

---

1. In Manage > Data Management > System Backup or Data Archive pages, select SCP or SFTP (Formerly FTP).
2. Enter the Host - The IP address or hostname of the host to receive the archived data.
3. Enter the Directory where the data will be stored:
  - For SCP - Specify the directory as an absolute path.
  - For SFTP - Specify the directory relative to the SFTP account home directory.
4. Enter the Port to use to send files over SCP or SFTP. The default port for SCP, SFTP, or SSH is 22. If the port is set to 0 (zero), the default port is in use (and you do not need to change it).
5. Enter the Username and Password - Credentials for the user that logs on to the SCP or SFTP server. This user must have write and execute permissions for the directory that is specified in Directory. For Windows, a domain user is accepted with the format of domain\user.  
Attention: For SFTP, the Username value cannot include any of the following characters: ! " \$ & ' () ; \ |
6. Optional: Schedule the backup in the lower part of the page. For more details, see [Scheduling](#).
7. Click Save.

### Related tasks

---

- [Configure data archive](#)
- [Archiving \(audit\) results](#)
- [Configuring system backup](#)

# Configure a Tivoli Storage Manager (TSM) archive or backup

Export to TSM (Tivoli Storage Manager) is not enabled by default. After you enable TSM, you can configure it for backups. Learn how to enable the service, and understand the configuration parameters that are used in the backup page.

## Before you begin

- Define a dsm.sys or dsm.opt configuration file on your server.
- For Tivoli Storage Manager (TSM) v7.1.8 or newer, you need a cert256.arm file. For more information, see [Configuring the server to use the cert256.arm certificate](#).

Note: The dsm.sys or dsm.opt file and cert256.arm file must be located in the same directory.

## About this task

Certificates are unique and cannot be reused on other Guardium servers.

## Procedure

1. Enable TSM backup from the Guardium CLI by entering:

```
store storage-system TSM backup on
```

2. Import the dsm.sys or dsm.opt configuration file by using the CLI command **import tsm config**.  
Guardium verifies the TSM version.

```
Is this Tivoli Storage Manager server <tsm server name> v7.1.8 or newer (y/n)?
```

If you are using TSM v7.1.8 or newer, type **y**. You are prompted to upload the cert256.arm file.

```
This appliance requires certificate authentication with <tsm server name>.
Is server certificate file ~/cert256.arm available now? (y/n)?
```

Type **y** to upload the certificate.

3. In **Manage > Data Management > System Backup**, select TSM.
4. Enter the Password, and reenter:
5. Select the Server:
6. Enter As host:
7. Optional: Schedule the backup in the lower part of the page. For more details, see [Scheduling](#).
8. Click Save.

## Related tasks

- [Configure data archive](#)
- [Archiving \(audit\) results](#)
- [Configuring system backup](#)

## Related information

- [store storage-system](#)
- [import tsm config](#)

## Internet Protocol modes

Configure Guardium® to run in a traditional IPv4-only environment, an IPv6-only environment, or in *dual mode* where the system supports both IPv4 and IPv6 addresses.

### IPv4 mode

IPv4 is the default mode of the Guardium system. This mode allows the system to communicate with devices that run over IPv4 only.

### IPv6 mode

If the IP mode is set to IPv6, Guardium supports only the databases, appliances, and other devices that are connected over IPv6.

### Dual mode

IPv4 and IPv6 are independent protocols and cannot communicate with each other.

The dual mode allows the Guardium system to communicate with devices that are running on IPv4, IPv6, or both.

#### Note:

The following Guardium features are not compatible with IPv6 mode and dual mode:

- Cloud database protection services
- IBM COS (Formerly Cleversafe) for archiving on external storage

The following third-party features and applications might not be compatible with IPv6 mode and dual mode. For more information, see the official website of the third-party.

- CyberArk
- Centera
- ECS 3.x or later
- ServiceNow
- z/OS versions earlier than 2.2

For information about using IPv6 with QRadar, see [IPv6 addressing in QRadar deployments](#).

- [Enable IPv4](#)

Configure your Guardium deployment to use IPv4 addresses exclusively.

- [Enable dual IP mode in an existing IPv4 deployment](#)

Configure your Guardium deployment to use both IPv4 and IPv6 addresses.

- [Migrate to IPv6 in an existing IPv4 deployment](#)

Configure your existing Guardium deployment to use IPv6 addresses exclusively.

- [Enable IPv6 in a new deployment](#)

Configure your new Guardium deployment to use IPv6 addresses exclusively.

- [Assign IPv6 addresses to your devices](#)

After you enable IPv6 in your central manager and managed units, assign the IPv6 protocol to all devices in your environment such as databases, and your Guardium agents, such as S-TAPs.

- [IPv6 limitations, best practices, FAQ, and troubleshooting](#)

---

## Enable IPv4

Configure your Guardium® deployment to use IPv4 addresses exclusively.

### Before you begin

IPv4 is the default IP mode for new Guardium installations and most existing deployments. Follow this procedure to configure IPv4 on systems that have been previously set to IPv6 or *dual mode*.

Warning: If you set the IP mode to IPv4, Guardium cannot communicate with systems running on other network protocols and any previous network settings are wiped out.

Ensure that you meet these prerequisites:

- All devices in your environment use IPv4 addresses. For example, the Guardium system and all Guardium agents, such as S-TAPs, are assigned IPv4 addresses.
- The Domain Name System (DNS) of your network is configured for IPv4.

### Procedure

1. On the central manager, set the IP mode to IPv4 by running the CLI command **store system ipmode ipv4**.

Important: Do not restart the network until you complete step 2.

2. Set up IPv4 by running the following CLI commands.

- a. **store system hostname <hostname>**

Where <hostname> can be resolved by the DNS for IPv4 addresses.

- b. **store system domain <domain name>**

Where <domain> is the domain name of your network.

- c. **store network interface ip <IP address>**

Where <IP address> is the primary IPv4 address of your Guardium system in Classless Inter-Domain Routing (CIDR) notation. For example, **store network interface ip 9.70.145.77/24**.

- d. **store network routes defaultroute <IP address>**

Where <IP address> is the IPv4 address of the default router.

- e. **store network resolvers <IP address>**

Where <IP address> is one or more IPv4 addresses for your DNS servers.

3. Restart the network configuration by running the CLI command **restart network**.

4. Verify that you can ping your Guardium system's IPv4 address.

5. Repeat steps 1 - 4 on each managed unit.

6. Register managed units to the central manager using the CLI command **register management <central manager IP> <port>** from each managed unit.

Where <central manager IP> is the IPv4 address of the central manager and <port> is the port number. For example, **register management 9.70.145.07 8443**. Repeat this step for each managed unit.

Important: To avoid connectivity issues during registration, use the IP address and not the hostname. To unregister a managed unit from a central manager, use the same IP mode and IP address that was used during registration.

7. After the central manager and managed units are configured, the environment is ready to register databases, devices, and other agents to the Guardium system using IPv4 addresses.

### Related concepts

- [Network Configuration CLI Commands](#)
- [Registering Units](#)
- [Unregistering a Managed Unit](#)

### Related information

- [store system ipmode](#)
- [restart network](#)

# Enable dual IP mode in an existing IPv4 deployment

Configure your Guardium® deployment to use both IPv4 and IPv6 addresses.

## Before you begin

**Dual mode** allows Guardium to communicate with devices using IPv4, IPv6, or both network protocols. Follow this procedure to enable *dual mode* on your central manager and register managed units using either IPv4 or IPv6.  
Attention: If your Domain Name System (DNS) supports multiple protocols, it can return either an IPv4 or IPv6 address for a specific hostname. If the returned IP address does not match the IP mode of the Guardium system, this can result in network connectivity issues. To avoid this scenario, use the IP address and not the hostname to connect a database, host, or device to the Guardium system.

Ensure that you meet these prerequisites:

- Your central manager and managed units are running Guardium V11.1 or later.
- Your network is configured to use Guardium over both IPv4 and IPv6.
- All devices in your environment use the appropriate protocol. For example, if you are using IPv6, the Guardium system and all Guardium agents, such as S-TAPs, are assigned IPv6 addresses. If you are using IPv4, the Guardium system and all Guardium agents, such as S-TAPs, are assigned IPv4 addresses.
- Each device is assigned a distinct hostname for each protocol. For example, a device that is running both IPv4 and IPv6 is configured with hostnames `devicename-IPv4` and `devicename-IPv6`.
- The DNS of your network is configured for IPv4 and IPv6.

## Procedure

1. On the central manager, set the IP mode to *dual mode* by running the CLI command `store system ipmode dual`.

Important: Do not restart the network until you complete step 2.

2. Set up IPv6 by running the following CLI commands.

This assumes that the central manager had a functioning IPv4 configuration before enabling *dual mode*. The following commands leave the existing IPv4 configuration intact while configuring the central manager for IPv6 connections.

- a. **store network interface ip <IP address>**

Where `<IP address>` is the primary IPv6 address of your Guardium system in Classless Inter-Domain Routing (CIDR) notation. For example, `store network interface ip 2002:0920:c000:3145:0000:0000:0000:0013/96`.

- b. **store network routes defaultroute <IP address>**

Where `<IP address>` is the IPv6 address of the default router.

- c. **store network resolvers <IPv4 address> <IPv6 address>**

Where `IPv4 address` is one or more IPv4 DNS addresses and `IPv6 address` is one or more IPv6 DNS addresses. When migrating an existing IPv4 deployment to *dual mode*, specify the same `IPv4 address` values used for the original IPv4 configuration.

3. Restart the network configuration by running the CLI command `restart network`.

4. Verify that you can ping your Guardium system's IPv4 and IPv6 addresses.

5. Enable IPv4 or IPv6 on each managed unit.

Follow the procedures to [Enable IPv4](#), [Enable IPv6 in a new deployment](#), or [Migrate to IPv6 in an existing IPv4 deployment](#).

6. After the managed units are set up in either IPv4 or IPv6 mode, register each managed unit to the central manager using the CLI command `register management <central manager IP> <port>` from each managed unit.

Where `<central manager IP>` is the IPv4 or IPv6 address of the central manager and `<port>` is the port number. For example, `register management 9.70.145.07 8443` for an IPv4 managed unit or `register management 2620:1f7:807:a000:920:8400:0:182 8443` for an IPv6 managed unit.

Important: To avoid connectivity issues during registration, use the IP address and not the hostname. To unregister a managed unit from a central manager, use the same IP mode and IP address that was used during registration.

7. After the central manager and managed units are configured, the environment is ready to register databases, devices, and other agents to the Guardium system using either IPv4 or IPv6 addresses.

## Related concepts

- [Network Configuration CLI Commands](#)
- [Unregistering a Managed Unit](#)

## Related information

- [store system ipmode](#)
- [restart network](#)

# Migrate to IPv6 in an existing IPv4 deployment

Configure your existing Guardium® deployment to use IPv6 addresses exclusively.

## Before you begin

Ensure that you meet these prerequisites:

- Your central manager and managed units are running on V11.1 or later.
- Your network is configured to use Guardium over IPv6.
- All devices in your environment use IPv6 addresses. For example, the Guardium system and all Guardium agents, such as S-TAPs, are assigned IPv6 addresses.

- The Domain Name System (DNS) of your network is configured for IPv6.

## About this task

---

Use this procedure to enable IPv6 on a central manager in an existing IPv4 environment.

Attention: If you set the IP mode to IPv6, Guardium cannot communicate with the systems that are running in IPv4 mode. Any previous network settings, including all IPv4 configurations, are wiped out.

## Procedure

---

- On the central manager, set the IP mode to *dual mode* by running the CLI command **store system ipmode dual**.

Important: Do not restart the network until you complete step [2](#).

- Set up IPv6 by running the following CLI commands.

- store network interface ip <IP address>**

Where <IP address> is the primary IPv6 address of your Guardium system in Classless Inter-Domain Routing (CIDR) notation. For example, **store network interface ip 2002:0920:c000:3145:0000:0000:0000:0013/96**.

- store network routes defaultroute <IP address>**

Where <IP address> is the IPv6 address of the default router.

- store network resolvers <IP address>**

Where IP address is one or more IPv6 addresses for your DNS servers.

- Unregister managed units by running the CLI command **unregister management** on each managed unit.

- Migrate each managed unit to *dual mode*.

- Set the IP mode to *dual mode* by running the CLI command **store system ipmode dual**.

Important: Do not restart the network until you complete step [4.b](#).

- Set up IPv6 by running the following CLI commands.

- store network interface ip <IP address>**

Where <IP address> is the primary IPv6 address of your Guardium system in Classless Inter-Domain Routing (CIDR) notation. For example, **store network interface ip 2002:0920:c000:3145:0000:0000:0000:0013/96**.

- store network routes defaultroute <IP address>**

Where <IP address> is the IPv6 address of the default router.

- store network resolvers <IP address>**

Where IP address is one or more IPv6 addresses for your DNS servers.

- Restart the network configuration by running the CLI command **restart network** on the central manager.

- Register managed units to the central manager using the CLI command **register management <central manager IP> <port>** from each managed unit.

Where <central manager IP> is the IPv6 address of the central manager and <port> is the port number. For example, **register management 2620:1f7:807:a000:920:8400:0:182 8443**. Repeat this step for each managed unit.

Important: To avoid connectivity issues during registration, use the IP address and not the hostname.

To unregister a managed unit from a central manager, use the same IP mode and IP address that was used during registration.

- After the central manager and managed units are configured, the environment is ready to register databases, devices, and other agents to the Guardium system using IPv6 addresses.

## Related concepts

---

- [Network Configuration CLI Commands](#)
- [Registering Units](#)
- [Unregistering a Managed Unit](#)

## Related information

---

- [store system ipmode](#)
- [restart network](#)

## Enable IPv6 in a new deployment

---

Configure your new Guardium® deployment to use IPv6 addresses exclusively.

## Before you begin

---

Warning: If you set the IP mode to IPv6, Guardium cannot communicate with systems running on other network protocols and any previous network settings are wiped out.

Ensure that you meet these prerequisites:

- Your central manager and managed units are running on V11.1 or later.
- Your network is configured to use Guardium over IPv6.
- All devices in your environment use IPv6 addresses. For example, the Guardium system and all Guardium agents, such as S-TAPs, are assigned IPv6 addresses.
- The Domain Name System (DNS) of your network is configured for IPv6.

## About this task

---

## Procedure

---

1. On the central manager, set the IP mode to IPv6 by running the CLI command **store system ipmode ipv6**.  
Important: Do not restart the network until you complete step 2.
2. Set up IPv6 by running the following CLI commands.
  - a. **store system hostname <hostname>**  
Where <hostname> can be resolved by the DNS for IPv6 addresses.
  - b. **store system domain <domain name>**  
Where <domain> is the domain name of your network.
  - c. **store network interface ip <IP address>**  
Where <IP address> is the primary IPv6 address of your Guardium system in Classless Inter-Domain Routing (CIDR) notation. For example, **store network interface ip 2002:0920:c000:3145:0000:0000:0000:0013/96**.
  - d. **store network routes defaultroute <IP address>**  
Where <IP address> is the IPv6 address of the default router.
  - e. **store network resolvers <IP address>**  
Where IP address is one or more IPv6 addresses for your DNS servers.
3. Restart the network configuration by running the CLI command **restart network**.
4. Verify that you can ping your Guardium system's IPv6 address.
5. Repeat steps 1 - 4 on each managed unit.
6. Register managed units to the central manager using the CLI command **register management <central manager IP> <port>** from each managed unit.  
Where <central manager IP> is the IPv6 address of the central manager and <port> is the port number. For example, **register management 2620:1f7:807:a000:920:8400:0:182 8443**. Repeat this step for each managed unit.  
Important: To avoid connectivity issues during registration, use the IP address and not the hostname. To unregister a managed unit from a central manager, use the same IP mode and IP address that was used during registration.
7. After the central manager and managed units are configured, the environment is ready to register databases, devices, and other agents to the Guardium system using IPv6 addresses.

## Related concepts

---

- [Network Configuration CLI Commands](#)
- [Registering Units](#)
- [Unregistering a Managed Unit](#)

## Related information

---

- [store system ipmode](#)
- [restart network](#)

## Assign IPv6 addresses to your devices

---

After you enable IPv6 in your central manager and managed units, assign the IPv6 protocol to all devices in your environment such as databases, and your Guardium® agents, such as S-TAPs.

## Databases

---

In the Datasource Definitions UI, update the datasource IP address in the Host Name/IP field.

## S-TAPs

---

1. If S-TAPs use numeric addresses for tap\_ip and sqlguard\_port, switch them to IPv6 format. Edit guard\_tap.ini, or use guard-config-update, for example.
2. These parameters might need modification, depending on the configuration:
  - Networks
  - exclude\_networks
  - connect\_to\_ip
  - alternate\_ips
  - load\_balancer\_ip
  - log4j\_listen\_address
3. Restart the S-TAPs.
4. Check connectivity to all databases and Guardium host systems.

## IPv6 limitations, best practices, FAQ, and troubleshooting

---

## Best practices

---

- Use a unique DNS name for every device and protocol on your network. For example, if you have a database server that supports both IPv4 and IPv6, it should have both an IPv4 DNS name and an IPv6 DNS name. For example, database-ip4.yourcompany.com and database-ipv6.yourcompany.com. This provides deterministic DNS lookups and prevents connectivity issues.
- Guardium systems only support one host name. When in *dual mode*, the system is registered to the DNS with the same host name for both IPv4 and IPv6. This can cause connectivity issues as the IP returned by the DNS could be IPv4 or IPv6. For example, if the central manager is in dual mode and you want to register a managed unit using IPv6, specify the IPv6 address of the central manager: **register management 2620:1f7:807:a000:920:8400:0:182 8443**.

To change the protocol used for registering a managed unit to the central manager, unregister the managed unit from the central manager, change its IP mode, then re-register it using the new IP format. For example, with a central manager in *dual mode* and a managed unit in IPv4, unregister the managed unit while it is in IPv4 mode, change its IP mode to IPv6, then re-register it to the central manager using an IPv6 address.

- Use Guardium host name aliasing to make reports easier to read. This feature works for both IPv4 and IPv6 protocols and uses DNS lookups for IP address aliasing.
- Configure infrastructure services like FTP to support IPv6.
- Use network tools and utilities that support IPv6. For example, the **ping** utility on some Linux and Windows system requires specifying the **-6** switch for IPv6 addresses (**ping -6 2620:1f7:807:a000:920:8400:0:182**), the **nslookup** utility requires specifying **-type=AAA** to resolve IPv6 host names (**nslookup -type=AAAA database-ipv6.yourcompany.com**), etc.

## Known limitations

---

### Changing to IPv4 or IPv6 mode from *dual mode*

If you are operating in *dual mode* and migrate to IPv4-only or IPv6-only mode, the network configuration for the IP protocol you did not migrate to is lost.

### Enterprise load balancing and *dual mode*

When using enterprise load balancing, a managed unit only supports the IP mode that was used for registering that managed unit to the central manager. This is true even if the collector is configured for *dual mode*. For example, if a managed unit in *dual mode* is registered to a central manager using IPv6, that managed unit cannot utilize IPv4. This limitation applies only to load balancing contexts with systems configured for *dual mode*.

### GDBI configuration

When migrating from IPv4 to IPv6 with an existing GDBI instance configured for IPv4, update the GDBI instance for IPv6 using the following GuardAPI command:

```
grdapic datamart_update_copy_file_info destinationHost=[<IPv6 address>] destinationPassword=<password>
destinationPath="/var/lib/sonargd/incoming" destinationUser="sonargd" transferMethod="SCP" Name=<datamart name>"
```

Issue this command on a central manager for each active datamart and allow the settings to sync to managed units.

### LDAP authentication configuration

When using LDAP for authentication configuration on the **Setup > Tools and Views > Portal** page, an IPv6 host address must be entered using brackets. For example: [2620:1f7:807:a000:920:8400:0:182].

### S-TAP `sqlguard_ip` parameter

If a Guardium collector has different networking information in DNS than what is configured on the system, S-TAP installations may have issues using a hostname for the `sqlguard_ip` parameter. To resolve this issue, align the DNS information and collector networking configuration. Otherwise, a numeric IP address can be specified for `sqlguard_ip`.

### S-TAP diagnostics

When the central manager is not on the same internet protocol as a Windows S-TAP, then the S-TAP diagnostics are not communicated to the central manager.

## Frequently asked questions

---

### How do you access a Guardium system using an IPv6 address?

Use square brackets for the IPv6 address in the URL. For example, [https://\[2620:1f7:807:a000:920:8400:0:182\]:8443](https://[2620:1f7:807:a000:920:8400:0:182]:8443)

### Why is it important to have unique names in DNS for the devices in my network?

Having unique DNS names makes DNS lookups deterministic. For example, if you have a database server that has the same name in DNS for IPv4 and IPv6, a lookup for that name may return either protocol. If that protocol is not used by the Guardium system, the connection will fail.

### The Guardium CLI only allows one hostname when configuring the system, but the IPv6 best practices indicate using unique host names for each IP protocol. Which hostname should I use when setting up a Guardium system in *dual mode*?

The name provided during host name setup is an internal configuration and is not used for networking configuration: it is used to help identify the system from the CLI and in reports. Any name can be used for this setting. For example, if you have a system configured with an IPv4 DNS name and an IPv6 DNS name, you can use either one.

### Why do you recommend using an IP address instead of a host name when registering managed units to a central manager?

In some environments, DNS is set up to have only one host name for both IPv4 and IPv6 addresses on the same device. In this case, using a host name does not guarantee which IP address is used and can lead to connection issues if one protocol is not supported. Therefore, when performing tasks such as registering managed units to a central manager, use the IP address of the protocol you want to use for the connection.

### I have both IPv4 and IPv6 databases on the same database server. How do I configure inspection engines on a collector running in *dual mode*?

Each internet protocol requires its own inspection engine. For a dual mode system, create both an IPv4 inspection engine and an IPv6 inspection engine.

### How do I determine which IP mode was used to register managed units to a central manager?

Use the **Reports > Guardium Operational Reports > Managed Units** report. The Managed Units report shows the host name and IP address of managed units: the IP address will be in either IPv4 or IPv6 format, depending on how the managed unit is registered to the central manager.

### I converted my collector to *dual mode*. Why is my S-TAP status red in the S-TAP monitor?

Verify that the S-TAP and collector are both communicating in the correct IP protocol. Use the **Manage > Activity Monitoring > S-TAP Control** page to confirm that the IP formats are the same. Expand the **Guardium Hosts** information for a specific S-TAP to review the collector information. If the S-TAP and collector are using different protocols, change the protocols to match.

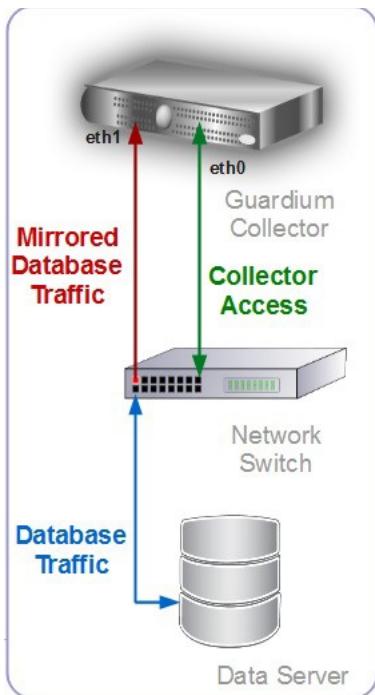
## Network mirroring methods (SPAN , N-TAP) and related inspection engines

---

This configuration is used in cases where an S-TAP cannot be installed in the host where the database instances to be monitored are run. Instead, you can direct a copy of the network traffic that goes to the host running the database servers, to a Guardium collector. This method only captures network traffic, not local traffic within the database server host. The limitations are listed further on in this section. IBM strongly encourages you to use an S-TAP instead.

**Port Mirroring:** For network traffic, you can use port mirroring, which is mirroring through SPAN (Switched Port Analyzer) ports. This requires a network switch with port mirroring capability. Physical setup and configuration of the inspection engine is required for port mirroring.

**Physical Setup:** The LAN containing the desktop used for connecting to the Guardium collector GUI should be connected to the eth0 port on the Guardium collector appliance. The SPAN port from the network switch should be connected to the eth1 port of the Guardium collector appliance. You can also connect additional SPAN ports to the remaining ethernet ports of the Guardium appliance, in order. The network switch must then be configured to mirror all traffic to and from the databases to be monitored, to a port on which the appliance is connected. A network administrator should be able to perform this configuration. You may need to consult the switch vendor's documentation for the exact process for setting up this configuration.



Since all network traffic from the host is sent to the collector, there can be potentially a high amount of useless (non-DB related) traffic the collector has to check before deciding to ignore it.

The collector needs to have a separate port for the incoming traffic from SPAN/NTAP. The actual setup is beyond the scope of Guardium (and Guardium support). Your network administrators are responsible for configuring this solution. Once the mirrored traffic is directed to the collector, you need to define inspection engines for each of the databases for which the traffic has been mirrored. Note that these inspection engine definitions are different from the definitions with the same name under S-TAP control.

For more information about creating and managing inspection engines, see [Configuring inspection engines](#).

## Related reference

- [update\\_engine\\_config](#)

## Configuring inspection engines

An inspection engine extracts SQL from network packets; compiles parse trees that identify sentences, requests, commands, objects, and fields; and logs detailed information about that traffic to an internal database.

You can configure, start, and stop multiple inspection engines on the Guardium® Data Protection appliance. You cannot create or run inspection engines on a central manager unit. However, you can start and stop inspection engines on managed units from the central manager control panel. After the inspection engine is configured, you can use the [update\\_engine\\_config](#) API to change the parameters.

You can define up to 50 inspection engines per Guardium appliance.

## Creating an inspection engine

1. Browse to [Manage > Activity Monitoring > Inspection Engines](#) to open the Inspection Engine Configuration page.
2. Click Add Inspection Engine to expand the panel.
3. Type a name in the Name box. It must be unique on the appliance. Guardium recommends that you use only letters and numbers in the name, as the use of any special characters prevents working with this inspection engine via the CLI.
4. From the Protocol box, select the protocol that you want to monitor from the list. Protocols are: Db2®, Informix, MSSQL, Mysql, Oracle, Sybase.
5. In the DB Client IP/Mask boxes, enter a list of clients (a client host from which the database connection was initiated) to be monitored (or excluded if the Exclude DB Client IP box is marked). The clients are identified by IP addresses and subnet masks. There are detailed instructions on how to use these fields in the overview.
  - Click the plus sign to add additional IP address and subnet mask.
  - Click the minus sign to remove the last IP address and subnet mask.
6. In the DB Server IP/Mask boxes, enter a list of database servers (where a database sits) to be monitored. The servers are identified by IP addresses and subnet masks. For information about identifying the IP addresses and subnet masks, see [Selecting IP addresses](#).
  - Click the plus sign to add additional IP address and subnet mask.
  - Click the minus sign to remove the last IP address and subnet mask.
7. In the Port box, enter a single port or a range of ports over which traffic between the specified clients and database servers will be monitored. Most often, this should be a single port.  
Warning: Do not enter a wide range of ports, just to be certain that you have included the correct one! You may cause the inspection engine to bog down attempting to analyze traffic on ports that carry no database traffic or traffic that is of no interest for your environment.
8. Mark the Active on startup box if this inspection engine should be started automatically on start-up.
9. Mark the Exclude DB Client IP box if you want the inspection engine to monitor traffic from all clients except for those listed in the DB Client IP/Mask list. Be sure that you understand the difference between this and the Ignore protocol selection. This includes all traffic except for the from IP addresses. To ignore a specific set of clients without including all other clients, define a separate inspection engine for those clients and use the Ignore protocol.

10. Click Add to save the definition.
11. Reposition the inspection engine in the list of inspection engines. Filtering mechanisms defined in the inspection engines are executed in the order. If necessary, reposition the new inspection engine configuration, or any existing configurations, using the Up and/or Down buttons in the border of the definition.
12. Click Start to start the inspection engine that you just configured. After the inspection engine starts, the Start button changes to Stop.

## Selecting IP addresses

---

Each inspection engine monitors traffic between one or more client and server IP addresses. In an inspection engine definition these are defined using an IP address and a mask. You can think of an IP address as a single location and a mask as a wild-card mechanism that allows you to define a range of IP addresses.

IP addresses have the format: n.n.n.n, where each n is an eight-bit number (called an octet) in the range 0-255.

For example, an IP address for your PC might be: 192.168.1.3. This address is used in the examples. Since these are binary numbers, the last octet (3) can be represented as: 00000011.

The mask is specified in the same format as the IP address: n.n.n.n. A zero in any bit position of the mask serves as a wildcard. Thus, the mask 255.255.255.240 combined with the IP address 192.168.1.3 matches all values from 0-15 in the last octet, since the value 240 in binary is 11110000. But it only matches the values 192.168.1 in the first three octets, since 255 is all 1s in binary (in other words, no wildcards apply for the first three octets).

Specifying binary masks can be a little confusing. However, for the sake of convenience, IP addresses are usually grouped in a hierarchical fashion, with all of the addresses in one category (desktop computers, for example) grouped together in one of the last two octets. Therefore, in practice, the numbers you see most often in masks are either 255 (no wildcard) or 0 (all).

Thus a mask 255.255.255.255 (which has no zero bits) identifies only the single address specified by IP address (192.168.1.3 in the example).

Alternatively, the mask 255.255.255.0, combined with the same IP address matches all IP addresses beginning with 192.168.1.

## Selecting all addresses

---

The IP address 0.0.0.0, which is sometimes used to indicate all IP addresses, is not allowed by Guardium. To select all IP addresses when using an IP address/mask combination, use any non-zero IP address followed by a mask containing all zeroes (for example: 1.1.1.1/0.0.0.0). However, 0.0.0.0/0.0.0.0 is a valid combination.

## Configure Settings that apply to all Inspection Engines

---

1. Go to Manage > Activity Monitoring > Inspection Engines to open the Inspection Engine Configuration.
2. Use the information in [Table 1](#) to make any needed changes.
3. Click Apply to save the updated system configuration when you are done making changes.  
Note: Any global changes made (and saved by using Apply) do not take effect until you restart the inspection engines. However, individual inspection engine attributes, such as exclude, sequence order, etc., take effect immediately.
4. Optionally add comments to the configuration.
5. Click Restart Inspection Engines to stop and restart all inspection engines.

You can also update the inspection engines by using the [update\\_engine\\_config API](#).

Note: The applied changes do not take effect until the inspection engines are restarted. After applying inspection engine configuration changes, click Restart to stop and restart the system (using the new configuration settings).

Note: The following inspection engine settings are not supported for HTTP: Default Capture Value; Default Mark Auto Commit; Log Sequencing; Log Exception Sql String; Log Records Affected; Compute Avg. Response Time; Inspect Returned Data; Record Empty Sessions.

Table 1. Settings that apply to all inspection engines

| Control                  | Description                                                                                                                                                                                                                                                                                                                                           |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default Capture Value    | Used by Replay function to distinguish between transactions and capture values, meaning that if you have a prepared statement, assigned values will be captured and replayed. If you want to replay your captured prepared statements as prepared statements the check box should be checked for the captured data.<br>Default value = false.         |
| Default Mark Auto Commit | Default value is true. Due to various auto-commit models for different databases, this value is used by Replay function to explicitly mark up the transactions and auto commit after each command.<br>Note: If the check box is checked then commits and rollbacks will be ignored. Databases currently supported include Db2, Informix®, and Oracle. |
| Log Sequencing           | If selected, a record is made of the immediately previous SQL statement, as well as the current SQL statement, provided that the previous construct occurs within a short enough time period.                                                                                                                                                         |
| Log Exception Sql String | If selected, when exceptions are logged, the entire SQL statement is logged.                                                                                                                                                                                                                                                                          |

| Control                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log Records Affected        | <p>Records affected - Result set of the number of records which are affected by each execution of SQL statements.</p> <p>The records affected feature is not supported in:</p> <ul style="list-style-type: none"> <li>• Db2 when streaming is used to send the results.</li> <li>• AWS</li> <li>• Couchbase</li> <li>• Hadoop integration</li> </ul> <p>If selected, the number of records affected is recorded for each SQL statement (when applicable). Default value for log records affected is FALSE (0).</p> <p>Note: The records affected option is a sniffer operation which requires sniffer to process additional response packets and postpone logging of impacted data which increases the buffer size and might potentially have a adverse effect on overall sniffer performance. Significant impact comes from really large responses. To prevent large amount of overhead associated with this operation, Guardium uses a set of default thresholds that allows sniffer to decide to skip processing operation when exceeded.</p> <p>Note: Usually, Records Affected is set correctly when the user turns on Log Records Affected via Inspection Engines &gt; Log Records Affected. However using MS-SQL via stored procedure will set Records Affected as -1.</p> <p>Refer to <a href="#">Configuration and Control CLI Commands</a> <code>store max_results_set_size</code>, <code>store max_result_set_packet_size</code> and <code>store max_tds_response_packets</code>, to set levels of granularity.</p> <p>Example of result set values:</p> <ul style="list-style-type: none"> <li>• Case 1, record affected value, positive number. This represents correct size of the result set.</li> <li>• Case 2, record affected value, -2. This means number of records exceeded configurable limit (This can be tuned through CLI commands).</li> <li>• Case 3, record affected value, -1. This shows any unsupported cases of packets configurations by Guardium.</li> <li>• Case 4, record affected value, -2. If the result set is sent by streaming mode.</li> <li>• Case 5, record affected value, less than -2. Intermediate result during record count to update user about current value, ends up with positive number of total records. For example, the server returns 1000 records in 4 packets: <ul style="list-style-type: none"> <li>◦ Packet #1 250</li> <li>◦ Packet #2 200</li> <li>◦ Packet #3 250</li> <li>◦ Packet #4 200</li> </ul> </li> </ul> <p>Then records affected are reported as</p> <ul style="list-style-type: none"> <li>◦ Packet #1 -250</li> <li>◦ Packet #2 -500</li> <li>◦ Packet #3 -750</li> <li>◦ Packet #4 1000</li> </ul> |
| Compute Avg Response Time   | When selected, for each SQL construct logged, the average response time is computed. 12.1 and later If the response time is longer than about 35 minutes (2 million milliseconds), the response time displays as -1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Inspect Returned Data       | Select to inspect data returned by SQL requests as well as update the ingress and egress counts.<br>If rules are used in the security policy, this checkbox must be selected.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Record Empty Sessions       | When selected, sessions containing no SQL statements are logged. When cleared, these sessions are ignored.<br>Note: This configuration works for other protocols, but not for Oracle Unified Auditing (OUA).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Parse XML                   | The Inspection Engine does not normally parse XML traffic. Mark this checkbox to parse XML traffic.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Logging Granularity         | The number of minutes (1, 2, 5, 10, 15, 30, or 60) in a logging unit. If requested in a report, Guardium summarizes request data at this granularity. For example, if the logging granularity is 60, a certain request occurred n times in a given hour. If the check box is not selected, exactly when the command occurred within the hour is not recorded. But, if a rule in a policy is triggered by a request, a real time alert can indicate the exact time. When you define exception rules for a policy, those rules can also apply to the logging unit. For example, you might want to ignore 5 login failures per hour, but send an alert on the sixth login failure.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Max. Hits per Returned Data | When returned data is being inspected, indicate how many hits (policy rule violations) are to be recorded.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Ignored Ports List          | A list of ports to be ignored. Add values to this list if you know your database servers are processing non-database protocols, and you want Guardium to not waste cycles analyzing non-database traffic. For example, if you know the host on which your database resides also runs an HTTP server on port 80, you can add 80 to the ignored ports list, ensuring that Guardium does not process these streams. Separate multiple values with commas, and use a hyphen to specify an inclusive range of ports. For example: 101,105,110-223                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Buffer Free: n %            | Display only. n is the percent of free buffer space available for the inspection engine process. This value is updated each time the window is refreshed. There is a single inspection engine process that drives all inspection engines. This is the buffer used by that process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Starting or stop an inspection engine

Browse to Manage > Activity Monitoring > Inspection Engines to open the Inspection Engine Configuration page.

- To start an inspection engine, click Start.
- To stop an inspection engine, click Stop.

## Removing an inspection engine

If you are no longer using an inspection engine, remove the definition, so that it is not accidentally restarted.

1. Click Manage > Activity Monitoring > Inspection Engines to open the Inspection Engines.
2. If the inspection engine you want to remove is still running, click Stop.
3. To remove an inspection engine, click Delete.

## Related reference

- [list\\_engine\\_config](#)
- [update\\_engine\\_config](#)

## Configuring the Guardium portal

From the Guardium Portal page, you can reset the port for the Guardium® appliance web server, import SSL certificates, and configure authentication for your Guardium system users.

To open the Guardium Portal page, click **Setup > Tools and Views > Portal**.

### Setting the port number

You can keep the Guardium appliance web server on its default port (8443) or reset the portal. Guardium recommends that you use the default port.

1. If not selected, select the Active on Startup checkbox (make sure that Active on Startup is always enabled).
2. Set the HTTPS Port to an integer value 1025 - 65535.
3. Click **Apply** to save the value. (The Guardium security portal does not start listening on this port until it is restarted.) Or click **Revert** to restore the value that is stored by the last **Apply** operation.
4. Click **Restart** to restart the Guardium web server if you made and saved any changes. You can now connect to the unit on the newly assigned port.

Note: To reconnect to the unit after it restarts with the new port number, change the URL that opens the Guardium Login page on your browser.

For more information about Guardium ports, see [Guardium port requirements](#)

### Importing SSL certificates

Use Import Certificate to import self-signed certificates with private keys.

Before you begin, generate certificates for each Guardium system, and store them locally.

Certificates can be generated in two formats:

- PKCS 12
- PEM

Note: After the certificates are imported, the GUI must be restarted for the changes to take effect.

- To import a PKCS 12 certificate:
  1. Select Import PKCS 12 certificate.
  2. Select Browse, and then browse to the certificate stored on your local system.
  3. In the **Password** field, enter your PKCS 12 file's password.
  4. In the **Certificate alias** field, enter the certificate's alias.
  5. Click **Import**. In the confirmation dialog, click Yes to restart the GUI. To restart the GUI later, click No.

Note: PKCS 12 certificates can be imported only through the GUI.

- To import a PEM certificate:
  1. Select Import PEM certificate.
  2. In the **PEM certificate** field, paste your certificate. Include the markers "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----".
  3. In the **PEM private key** field, paste your certificate's key. Include the markers "-----BEGIN RSA PRIVATE KEY-----" and "-----END RSA PRIVATE KEY-----".
  4. Click **Import**. In the confirmation dialog, click Yes to restart the GUI. To restart the GUI later, click No.

Note: You can also import PEM certificates from the CLI. For more information, see [Store certificates with private key](#).

### Configuring authentication

Authentication defines the way user passwords are authenticated when users log in to the Guardium appliance. From the Portal page, select one of the following authentication configurations:

- Local (the default) - A login and password for a specific user is defined from the accessmgr role on the Guardium accessmgr account.
- RADIUS - Allow login authentication through a Radius server. The Radius/RSA server is defined by using both a password and a SecurID token number. The SecurID token numeric password is displayed on a hardware token.
- LDAP - Allow login authentication when the password is defined and stored on a specified lightweight directory access protocol (LDAP) server.
- Smart Card - Require login to the Guardium UI using a smart card.
- Single sign-on SAML - Allows access to multiple web-based applications using one set of login credentials.

For more information about user authentication, see [Configuring authentication](#). For more information about smart card authentication, see [Enabling smart card authentication](#).

### Configuring multi-factor (two-factor) authentication

Multi-factor (or two-factor) authentication (MFA) adds an extra layer of security to your Guardium user accounts. Guardium supports DUO and RSA SecurID authentication engines. For more information about configuring your system for multi-factor authentication, see [Configuring multi-factor authentication](#).

- [Configuring authentication](#)  
By default, Guardium user logins are authenticated by Guardium, independent of any other application.
- [Enabling smart card authentication](#)  
Guardium smart card support meets the United States government mandate that all vendors must support multi-factor authentication for user access. Smart card authentication is supported only for access to the web-based Guardium user interface (UI).

- [Configuring multi-factor authentication](#)

Multi-factor (or two-factor) authentication (MFA) adds an extra layer of security to your Guardium user accounts.

## Configuring authentication

By default, Guardium® user logins are authenticated by Guardium, independent of any other application.

For the Guardium admin user account, login is always authenticated by Guardium alone. For all other Guardium user accounts, authentication can be configured to use RADIUS, LDAP, a smart card or Single sign-on SAML. Extra configuration information is required for connecting with the authentication server.

When using RADIUS or LDAP, all Guardium users must still be defined as users on the Guardium appliance. It is only the authentication that is performed by another application.

While user accounts and roles are managed by the accessmgr user, the authentication method used is managed by the admin user, which is a standard separation-of duties best practice.

In addition, you can also authenticate users with a smart card and for any authentication method, add a level of security with multi-factor authentication. For more information, see [Enabling smart card authentication](#) and [Configuring multi-factor authentication](#).

To set up user authentication from the Portal:

1. Browse to Setup > Tools and Views > Portal.
2. From Authentication Configuration, select the type of authentication you want to use.  
Note: Local is the default.
3. Configure the authentication type as required.

## Configuring Guardium local authentication

Select Local (the default) to define logins and passwords for specific users from the access manager (that is, the accessmgr role on the Guardium accessmgr account). For more information about accessmgr, see [Managing users](#).

When you define a username and password from the accessmgr role, the defined password per user is used to log in to the Guardium system.

To configure Guardium for local authentication, select Local and click Apply.

## Configuring RADIUS authentication

Select RADIUS to allow login authentication through a Radius server. The Radius/RSA server is defined by using both a password and a SecurID token number. The SecurID token numeric password is displayed on a hardware token.

You can define the Radius/RSA server on either a Windows or UNIX server. The security RSA SecurID token is defined and stored on the Radius server. You do not need to download it for the Radius portal to work.

Guardium supports FreeRADIUS client software. To use FreeRADIUS, the client (Guardium server), username, and passwords are defined on the FreeRADIUS UNIX servers and used when the Radius Portal connection is defined.

1. Select RADIUS in the Authentication Configuration page to display the RADIUS-specific fields. Enter the following information for RADIUS:
  - a. Primary Server - The hostname or IP address of the primary RADIUS server.
  - b. Secondary Server and Tertiary Server - Optionally enter the hostname or IP address of the secondary and tertiary RADIUS servers.
  - c. Port The UDP port used (1812 or 1645) by RADIUS.
  - d. Shared Secret - Enter the RADIUS server Shared Secret, twice.
  - e. Timeout Seconds - The number of seconds before the server times out (the default is 120).
  - f. Auth Type - Select an authentication type:
    - PAP - Password authentication protocol
    - CHAP - Challenge-handshake authentication protocol
    - MS-CHAPv2 - Microsoft version 2 of the challenge-handshake authentication protocol
2. Click Test to verify the configuration. You are informed of the results of the test. The configuration is also tested whenever you click Apply to save changes.
3. Click Apply. Guardium attempts to authenticate a test user, and informs you of the results.

## Configuring LDAP authentication

LDAP authentication allows login authentication when the password is defined and stored on a specified lightweight directory access protocol (LDAP) server. A user account name must be imported from the LDAP server to allow a user to use the LDAP portal and to log in.

Guardium supports multiple LDAP servers. The access manager defines the LDAP configurations, which display in the LDAP servers table under Authentication Configuration. For more information about defining the LDAP configurations, see [Importing users from LDAP](#).

Note: Default User RDN Type defines the default value of User RDN Type. If you add a new LDAP server for user import, the User RDN Type attribute is populated with the value defined here.

If you configure Default User RDN Type with the <LDAP Attribute>=search, Guardium applies an additional filter (<LDAP Attribute>=<username>). Guardium searches for the user DN and then authenticates the user with the resultant DN.

For example, let's say that you configure User RDN Type as uid=search, when a user logs in (Hadrian Wall for example), Guardium applies the additional filter (uid="home\_markdown\_jenkins\_workspace\_Transform\_in\_SSMPHH\_12.x\_com.ibm.guardium.doc.admin\_config\_configuring\_authentication\_HadrianWall") and searches for the user DN in LDAP. If Guardium finds "HadrianWall," then Guardium uses the DN and the supplied password to authenticate with the LDAP server.

Note: If the user RDN type for your site is not uid, then work with your access manager to establish the user RDN. The access manager imports LDAP users and can tell you which RDN to use as the default.

After the access manager configures LDAP authentication, you can optionally choose to add or view trusted certificates or test the authentication. When you are done, click Apply to finish the set up, as described in step 4.

1. Optional. To inspect one or more trusted certificates, click Trusted Certificates and follow the instructions in that window.
2. Optional. To add a trusted certificate, click Add Trusted Certificates and follow the instructions in that window.  
Note: If multiple LDAP servers use SSL, you need to add an SSL certificate for each server. However, if the certificates are signed by the same certificate authority, you can add only the root certificate.
3. Optional. Click Test to verify the configuration and return the results. The configuration is also tested whenever you click Apply to save changes.
4. Click Apply. Guardium attempts to authenticate a test user, and informs you of the results.

## Enabling smart card authentication

---

You can configure Guardium smart card support that meets the United States government mandate that all vendors must support multi-factor authentication for user access. Smart card authentication is supported for access to the web-based Guardium user interface (UI). For more information about smart card authentication, see [Enabling smart card authentication](#).

## Single sign-on SAML authentication

---

Single sign-on SAML is an authentication process that allows access to multiple web-based applications that use one set of login credentials.

Before you set up SAML authorization on the Guardium appliance, you need to have your identity provider (IDP) metadata file that is provided by your company. This file contains a public certificate that communicates with the Guardium appliance. More information on the IDP can be found of your companies help page.

1. Click Single sign-on (SAML) and then click Configure. The Configure SAML authentication window is displayed.
2. Enter the following information in the Configure SAML authentication window:

### Browse

Select an XML-format file that contains an IDP certificate.

### Request binding protocol

Depending on your IDP, select the correct protocol:

- HTTP-Redirect - Communicates through URL parameters given.
- HTTP- Post - Communicates through messages based on Base64 encoding.

### Request signed assertion

Select Yes if you want the IDP to sign the SAML assertion that is sent back to the Guardium Appliance. An assertion contains a package of information about a user and their authentication status and XML attributes.

### Request encrypted assertion

Select Yes to encrypt the assertion that is given to the Guardium appliance.

### Sign authentication requests

Select Yes to have Guardium sign the SAML request sent to the IDP.

### Enable service provider initiated single logout

Select Yes to be signed out of the IDP whenever logout is initiated. Your response depends on whether this feature is supported by your IDP.

### Certificate for signing and encryption

Select guardium\_default or click  to add your own PEM-formatted certificate.

### How to authorize

Select one of the following parameters:

- Local - Allows authorization for local users on the Guardium appliance. These local users are manually created and added into the Guardium appliance.
- User attribute - Allows authorization for users from the LDAP in the IDP. Searches for specific attributes that are returned from the SAML assertion.

You can choose one or more of the following attributes:

- Role attribute - Assigns permissions to the user based on the Guardium role
- First name attribute
- Last name attribute
- Email attribute

3. Click Generate SP metadata to generate a metadata file using the given data.

4. Click Save to save your changes and close the Configure SAML Authentication window. After saving, the metadata file is automatically downloaded and can then be uploaded to your IDP. You are now back to the Authentication Configuration screen.

5. Click Apply to save your changes. Reconfiguration of SSO can happen without needing to click again.

Tip: Admin and accessmgr users can log into the Guardium system without using SAML authentication. For more information, see the CLI command [store system admin-only](#).

## Related concepts

---

- [Importing users from LDAP](#)
- [Configuring multi-factor authentication](#)

## Related tasks

---

- [Enabling smart card authentication](#)

## Enabling smart card authentication

---

Guardium smart card support meets the United States government mandate that all vendors must support multi-factor authentication for user access. Smart card authentication is supported only for access to the web-based Guardium user interface (UI).

## Before you begin

---

Details of the multi-factor authentication requirement are found in the Identification and Authentication (Organizational Users) (IA-2) section the Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53) document. NIST 800-53 is available through the NIST website: <https://www.nist.gov>.

Government applications refer to Personal Identification and Verification Cards (PIV). Civilian applications refer to Common Access Cards (CAC). PIV and CAC cards have different certificate authorities, but the cards are otherwise the same.

Guardium smart card support meets the HIGH confidence PIV assurance level. PIV assurance is described in the PIV Cardholder Authentication (6) section of the Personal Identity Verification (PIV) of Federal Employees and Contractors (FIPS Publication 201-2) document. FIPS 201-2 is available through the NIST website: <https://www.nist.gov>.

In addition to the configuration steps described here, users require,

- Access to the Guardium UI from a web browser that can access the smart card certificate.
- A valid PIV or CAC card.
- A smart card reader.

Tip: Admin and accessmgr users can log into the Guardium® system without using a smart card. For more information, see the CLI command [store system admin-only](#).

You can either associate existing Guardium users or create users to associate with smart cards. You can also import user definitions from an LDAP server and edit the smart card user name field without losing any related settings. After you configure your site to use smart card for authentication, Guardium uses the smart card credential only to establish SSL/TLS communication (Guardium uses HTTPS). For more information about creating users and access management, see [Managing access to Guardium](#). Note: While smart card authentication is used to authenticate, you still need to set user access control (that is, which Guardium modules a user can access) through access management.

## About this task

This task describes how to associate the information on a smart card with a Guardium user.

## Procedure

1. Log in as Admin from a central manager or standalone machine.
2. Browse to Setup > Tools and Views > Portal.
3. From Authentication Configuration, select Smart Card.
4. In Regex Match Pattern, use a regular expression (regex) to match the user information on the smart card, for example,

```
CN ?= ?(.*)?, ?OU ?= ?Test Agency, ?OU ?= ?Test Department, ?O ?= ?Test Government, ?C ?= ?US
```

In this example, both patterns match the mapping for the client certificate. Pattern 1 is more exact, but with pattern 2, you can edit the pattern to match your needs. If you are not familiar with the data on the smart card, work with someone who can write efficient mapping patterns.

- Pattern 1:

```
CN ?= ?(.*)?, ?OU ?= ?Test Agency, ?OU ?= ?Test Department, ?O ?= ?Test Government, ?C ?= ?US
```

- Pattern 2:

```
CN ?= ?.*?
```

Both of the examples get the value for CN attribute in the certificate subject (which you can see by examining the certificate details in the browser). Configuring this pattern correctly is probably the most important step in making sure that smart card authentication is successful.

Note: The Guardium regex validation tool cannot validate the regex for smart card.

Tip: You can update the regex values for smart card authentication with the SMART\_CARD\_MAPPING\_REGEX parameter of the **modify\_guard\_param** API command. For more information, see [Smart card parameter](#).

5. Upload or add a trusted certificate from a certificate authority (CA) to your web server truststore.

You can obtain a certificate either directly from a customer or by exporting it from a smart card by using a certificate management tool such as certMgr.exe or OpenSSL.

Note: If you do not have the root certificate of the CA that signed the certificates on the smart cards, export a root certificate from a CA-signed user certificate or a smart card that contains one.

Important: If you enable Online Certificate Status Protocol (OCSP) validation, you must upload valid OCSP client certificates. If the client certificates are not OCSP-enabled, you cannot access the Guardium system and the admin user cannot revert the setting. Valid OCSP certificates indicate Method #1: Online Certificate Status Protocol and include a valid URI

- a. If trusted certificates are available, click Trusted Certificates.

Select a certificate to use for smart card authentication. The signing chain lists a series of signing authorities. The best certificate to select is usually the intermediate authority above the user certificate.

- b. If you do not have a certificate available, click Add Trusted Certificates and then browse to the certificate location and click Upload to import the certificate.

In general, you want to import the public root certificate of a trusted CA. This is the most common source of a root certificate in environments that already have a smart card infrastructure and a standardized approach to smart card distribution and authentication.

6. If needed, select Enable OCSP check to enable OCSP validation.

When the OCSP check is enabled, Guardium communicates with the OCSP responder ensures that the certificate in the truststore is valid. If the certificate is unknown or revoked, a user receives an error message when they attempt to log in to Guardium.

Note: Upload the OCSP-enabled certificates before you select Enable OCSP check.

7. Click Save to save your work. However, you aren't finished yet. You still need to distribute the authentication configuration to managed units on your network and then enable smart card authentication from the CLI.

8. On a central manager, browse to Manage > Central Management > Central Management.

- a. On the Central Management page, select the managed units that you want to include for smart card authentication.

- b. Click Distribute Authentication Config and then check the results to make sure that the selected managed units were updated successfully.

- c. Distributing the authentication configuration to the managed units can take up to an hour. To distribute the authentication configuration immediately, click Refresh.

9. Next, turn on smart card authentication from the Guardium CLI.

To turn smart card authentication on or off, use the following CLI command,

```
store system websmartcard [on | off]
```

Note: Whenever you run this CLI command, the GUI automatically restarts. When you disable smart card authentication, the GUI restarts with the system that uses local authentication.

To check the status of smart card authentication, use the following CLI command,

```
show system websmartcard
```

For more information, see [store websmartcard](#) in [System CLI commands](#).

10. Optional: The admin or accessmgr can log into the Guardium system without a smart card by using a separate login page.

Run the CLI command **store system admin-only on**. Then, access the login page by appending /admin to the URL of your Guardium system. Example: *https://www.[your\_guardium\_system's\_domain\_name].com:[port\_number]/admin*. Log in using your credentials.

For more information, see [store system admin-only](#) in [System CLI commands](#).

## What to do next

---

After smart card authentication is enabled, you can access the site with a valid smart card (such as PIV or CAC). Enter the card into the card reader. Depending on how your smart card is configured, you might be asked to enter the PIN associated with the smart card.

After you swipe the smart card:

1. A list of certificates displays. Select a certificate from the list.
2. If requested, enter your PIN.
3. If Guardium recognizes the smart card certificate, the Guardium dashboard opens. If the certificate is invalid (or revoked), the user receives an authentication error.

### Troubleshooting

- After you enable smart card authentication, you get an error from the Guardium URL.

Diagnosis: Most likely, your configuration of the matching regular expression is incorrect or you don't have a valid certificate on the card.

- You created a matching regex and it does not seem to be working. You know that Guardium has a regex validation tool and use it, thinking that if it works in the tool, it's a good regex pattern. Unfortunately, while the test is successful in the tool, the regex pattern doesn't work for smart card configuration.

Diagnosis: The regex tool determines if regex can find an expression inside a text paragraph. When configuring a smart card, regex extracts a piece of text from the certificate (displayed in the subject as shown in certificate details), and therefore does not work in this situation.

- You didn't get prompt from the browser to select a certificate.

Diagnosis: Your computer is able to install the card reader and the smart card. A copy of the certificate in the smart card is copied to the certmgr in Windows OS. However, the browser (such as Firefox or Chrome) cannot read the certificate. In other words, browsers on Windows are unable to read the certificate and there is no prompt to choose the certificate.

This is a rare, but known, situation on all browsers on some laptops that were tested. In this case, the issue is with your smart card configuration and not Guardium.

Solution: Contact your smart card administrator.

## Related concepts

---

- [Portal configuration](#)
- [System CLI commands](#)

## Related information

---

- [Smart card parameter \(modify\\_guard\\_param\)](#)

## Configuring multi-factor authentication

---

Multi-factor (or two-factor) authentication (MFA) adds an extra layer of security to your Guardium user accounts.

## Multi-factor (two-factor) authentication configuration

---

Guardium supports DUO and RSA SecurID authentication engines.

To start configuring an authentication service, click Configure to open the Configure multi-factor authentication window. Select an authentication service, and click Save to view the settings for the selected service.

For more information about using DUO, see [Configuring multi-factor authentication with DUO](#).

For more information about using RSA SecurID, see [Configuring multi-factor authentication with RSA SecurID](#).

## Configuring multi-factor authentication with DUO

---

To enable multi-factor authentication for DUO on Guardium, your site needs a DUO administrator. For more information, see <https://duo.com/product/multi-factor-authentication-mfa>. After you install DUO, you can enable MFA for your GUI, your CLI, or both. In addition, you can create a list of users who are exempt from additional authentication.

Note: To use MFA, the user's web browser (for GUI) or gmachine (for CLI and SSH) must have access to the DUO cloud service for MFA. If the DUO cloud service is not reachable (via the internet), then the user cannot be authenticated (and cannot log in).

To use MFA with DUO in a centrally managed environment, you must set up MFA on the central manager. The MFA configuration is automatically synchronized to all of its managed units.

Note: Even though you can set or change MFA authentication only from the central manager, you can query the configuration from any associated machine.

Note: If you unregister a managed unit in a centrally managed environment, the MFA settings for the unregistered unit are disabled.

1. Determine which users require MFA. You can configure MFA for GUI users, regular CLI users (that is, CLI users that are created by the accessmgr), or administrative OS users (cli and guardcli1 - guardcli9 users). Before you configure Guardium®, you need to protect the application with DUO:
  - For the GUI, protect the Web SDK.
  - For the CLI, protect the DUO Auth API.
  - For SSH, protect the UNIX application. You can configure each DUO application as needed. For more information, see the DUO documentation.
2. Within DUO, configure your users for authentication.

After you set up protection in DUO, you can configure multi-factor authentication in Guardium.

1. From the Guardium UI, click Configure next to Multi-factor Authentication.
2. From the Configure multi-factor authentication window, select DUO as the service.
3. To configure the GUI for MFA,
  - a. From the GUI login tab, select Enable multi-factor authentication for GUI logins.
  - b. Copy the Integration key, Secret key, and API hostname from DUO Web SDK application.
  - c. Click Save.
4. To configure the CLI for MFA,
  - a. From the CLI login tab, select Enable multi-factor authentication for CLI logins.
  - b. Copy the Integration key, Secret key, and API hostname from DUO Auth API application.
  - c. Click Save.

For more information about logging in to the CLI with multi-factor authentication, see [Using GuardAPI commands](#).
5. To configure SSH users for MFA,
  - a. From the SSH login tab, select Enable multi-factor authentication for SSH logins.
  - b. Copy the Integration key, Secret key, and API hostname from the UNIX application.
  - c. Click Save.

Note: SSH login supports only password-based authentication with MFA. If your site uses certificate-based authentication, the MFA settings are ignored.
6. To add exempt users,
  - a. On the Exemptions tab, all of the users on your system display (including disabled users and users imported from the LDAP server).
  - b. Select the users who you want to exempt from MFA. Exempt users might include accessmgr, admin, and selected trusted users.
  - c. Click Save to add the users to the exempt list.

Note: You cannot exempt administrative OS users (cli and guardcli1 - guardcli9).

When non-exempt users next login, they are asked to authenticate based on your configuration selections in DUO.

Note: You can use GuardAPIs or REST APIs to manage multi-factor authentication. For more information, see [Multi-factor authentication APIs](#).

## Configuring multi-factor authentication with RSA SecurID

Your site can use MFA with RSA SecurID for Guardium GUI users, regular CLI users (that is, CLI users who are created by the accessmgr), or SSH users (cli and guardcli1 - guardcli9 users). Before you can use RSA SecurID for multi-factor authentication, you need to install and configure the RSA Authentication Manager on a central manager or stand-alone machine.

Note: When you install RSA Configuration Manager, you must enable the RSA SecurIDAuthentication API. When you enable the API, RSA SecurID generates and displays the Access Key. Copy the Access Key value to a secure location where you can access it when you configure the authentication agents later.

For more information, see the RSA SecurID documentation about configuring the RSA SecurID Authentication API.

RSA SecurID uses token-based authentication. The token is either generated on a hardware key fob or as a software token. You can use either token type for MFA with Guardium.

For more information about RSA SecurID and the RSA Authentication Manager, see "Getting Started with RSA Authentication Manager" from the RSA website.

Note: If you plan to require MFA for SSH users, you need a signed SSL certificate from a trusted certificate authority (CA). The certificates are not required for GUI and CLI users. The certificate must be in PEM format, for example, `rsa_cert.pem`.

When you configure Guardium, you can upload the certificate either by using the `store certificate rsa_securid` CLI command or from the Configure multi-factor authentication page.

To configure RSA SecurID on a Guardium central manager, log in to the RSA security console, and then take the following steps,

1. Add users to RSA SecurID. From the RSA security console, select Identity->Users->Add New.
2. If your site uses software tokens, determine the authentication type that you want to use, and add a software token profile. Select Authentication->Software Token Profiles->Add New. For more information about managing software tokens, see the RSA SecurID documentation.

Note: If your site uses hardware tokens, do not create a software token profile.
3. Assign tokens to users,
  - a. From the RSA security console, select Identity->Users->Manage Existing.
  - b. Click Search to display all of the available users. Leave the search criteria empty to display all users.
  - c. Click a username and then select SecurID Tokens from the drop-down list.
  - d. Select a token from the available tokens list and click Assign. A message displays when a token is assigned.
  - e. Click Cancel to return to the Manage Existing page and assign tokens to other users.
4. Set up the authentication agent,
  - a. From the RSA security console, browse to Access->Authentication Agents->Add New.
  - b. Add a new, unique, hostname for the Guardium machine to which you want to authenticate. The Guardium host can be either a central manager or a managed unit. After you enter the hostname, click Resolve Hostname; the IP address is automatically entered.
  - c. Copy and save the hostname. You will need to enter it in Guardium as the Client ID.
  - d. You can keep the default settings or change the settings as needed and then click Save.
5. If you did not save the Access Key earlier, you can find the value from the RSA security console System Settings window,
  - a. Browse to Setup->System Settings. Under Authentication Settings, click RSA SecurID Authentication API.
  - b. Copy the value of the Access Key to a secure location.

## Configuring RSA SecurID authentication on Guardium

After the RSA SecurID console is configured, you can configure RSA SecurID on Guardium. Each user requires their own client ID and access key (or token). In addition, you can create a list of users who are exempt from additional authentication.

To enable MFA, you need the following information from the RSA SecurID Authentication Manager:

- Hostname: The hostname of the RSA SecurID Authentication Manager. The hostname is usually a fully qualified domain name.
- Port: The port that RSA SecurID Authentication Manager uses for the authentication service. The default is 5555.
- Client ID: The hostname of the authentication agent that you added to the RSA SecurID security console in Step 4 of [Configuring multi-factor authentication with RSA SecurID](#).
- Access key: The access key that is generated from the RSA SecurID Authentication API. You can find the value of the Access key in the RSA SecurID Security Settings, as described in Step 5 of [Configuring multi-factor authentication with RSA SecurID](#).

In addition, you can include a signed SSL server certificate. Select Validate server certificate and then click Upload certificate. Browse to the location of the certificate and click Open.

Note: A signed certificate, in PEM format, is required for SSH logins only.

To add exempt users,

1. On the Exemptions tab, all of the users on your system display (including disabled users and users imported from the LDAP server).
2. Select the users who you want to exempt from MFA. Exempt users might include accessmgr, admin, and selected trusted users.
3. Click Save to add the users to the exempt list.

Note: You cannot exempt administrative OS users (*cli* and *guardcli1 - guardcli9*).

When non-exempt users log in to Guardium, they need to provide a passcode from RSA SecurID. The passcode is either generated on the user's RSA SecurID hardware fob (token) or from the RSA SecurID software token on the users computer or phone.

## Logging in to Guardium with RSA SecurID MFA

---

To log in to Guardium as a user in an environment with RSA SecurID MFA, you need to either acquire a hardware token from your RSA SecurID or download the RSA SecurID software token.

Follow your administrator's instructions for installing the RSA SecurID token. After you have a token (either software or hardware) and MFA is configured for Guardium, you will need to provide a token passcode whenever you log in.

When a passcode is requested, copy the passcode and paste (or type) it into the Passcode box (for the UI) or at the Enter passcode prompt (for the CLI).

Depending on how your environment is configured, you might need to provide a passcode to log in to the GUI, the Guardium CLI, or both.

---

## Managing the TLS version

Use APIs to manage TLS 1.2 and TLS 1.3 protocols for your appliances, S-TAP agents, CAS and GIM clients. As you update your Guardium system to Guardium 12.0, you can enable TLS 1.3 and disable TLS 1.2.

## Before you begin

---

Updating your Guardium configuration to transport layer security (TLS), 1.3 provides a faster and more secure encryption protocol. However, TLS 1.3 runs only on Guardium 12.0 or later. For systems in transition, where you have appliances and S-TAPs that use different versions of Guardium, you can use both TLS 1.2 and TLS 1.3. When you install or upgrade to Guardium 12.0 or later, TLS 1.2 and TLS 1.3 are enabled by default.

Note: You can enable TLS 1.3 only on appliances, the GIM client, and S-TAPs that are at Guardium 12.0 or later. While you can, for example, use a Guardium 12.0 central manager (with TLS 1.3 enabled) along with earlier versions of Guardium for the managed units and S-TAPs (with TLS 1.2 enabled), Guardium recommends that you bring all of your appliances to Guardium 12.0 or later so that you can enable TLS 1.3 across your entire Guardium system.

Note: As you prepare to upgrade to Guardium 12.0, all of the appliances, agents, and so on that you plan to upgrade must have TLS 1.2 enabled. Make sure that all of the systems that you plan to upgrade have TLS 1.2 enabled. For information about upgrading to TLS 1.2 on a pre-12.0 system, see [Managing the TLS version](#) in IBM Docs for your (pre-12.0) version of Guardium.

Important: While Guardium supports TLS 1.3, not all add-ons and features currently provide TLS 1.3 support. Until you know that every part of your Guardium system supports TLS 1.3, do not disable TLS 1.2 (that is, do not run the [enable\\_latest\\_tls](#) API on your central manager). The following add-ons and features support only TLS 1.2:

- External ticketing with IBM Resilient. For more information about IBM Resilient, see [Configuring an external ticketing system](#).
- External ticketing with ServiceNow. For more information about ServiceNow, see [Configuring an external ticketing system](#).
- Running CAS in FIPS mode. To run in FIPS mode, the CAS client requires IBM Java 8 SR7 or later. For more information about configuring CAS, see [Prerequisites, installing and running CAS on a Linux, UNIX server](#) or [Prerequisites, installing, and running CAS on a Windows server](#).
- In most cases, both TLS 1.2 and 1.3 support FIPS 140 mode. However, under some circumstances, you must disable TLS 1.3 before you can enable FIPS 140 mode. For more information, see [enable\\_fips\\_tls](#).
- Guardium® Data Protection does not support TLS 1.3 on Solaris operating system from version 12.0 and later.
- Guardium Data Protection does not support FIPS 140-3 on Solaris operating system from version 12.1.

## Procedure

---

1. Access the CLI as admin.
2. Determine the versions of your central manager, managed units, and GIM client.

You can run one of the following commands to find the current versions of the TLS that are enabled on your system:

- Run the `show tls enabled` CLI command to see which TLS versions are enabled.
- Run the `grdapi get_secured_protocols_info` API from a central manager to propagate down to all managed units. The command displays the enabled protocols (TLS 1.2 and TLS 1.3) and indicates if the TLS 1.2 protocols can be disabled.  
Messages display to indicate which components do not meet the requirements for disabling TLS 1.2. Warning messages are generated for managed units that are offline or unreachable.

For more information, see [show tls enabled](#) and [get\\_secured\\_protocols\\_info](#).

3. Depending on the status of your system, take one of the following steps:
- To enable TLS 1.3, and optionally disable TLS 1.2, run the following command:  
`grdapi enable_latest_tls`

- To enable both TLS 1.2 and TLS 1.3, run the following command:  
`grdapi enable_all_tls`

For more information, see [enable\\_all\\_tls](#) and [enable\\_latest\\_tls](#).

## Related reference

---

- [enable\\_all\\_tls](#)
- [enable\\_fips\\_tls](#)
- [enable\\_latest\\_tls](#)
- [get\\_secured\\_protocols\\_info](#)

## Related information

---

- [show\\_tls\\_enabled](#)

## Global profile

---

The Global Profile page defines defaults that apply to all users.

## Getting started with the global profile

---

To open the Global Profile page, browse to Setup > Tools and Views > Global Profile.

Use the Global Profile page to set defaults for your Guardium® system. You can add your own header and footer to reports, upload your company logo, create a default message template, and much more.

Note: Whenever you change information on the Global Profile, you need to scroll to the end of the page and click **Apply** for the change to take effect.

## Changing settings for aliases and PDFs

---

You can change the following settings for aliases and PDF footers:

- Use aliases in reports unless otherwise specified: An alias provides a synonym that substitutes for a stored value of a specific attribute type. Aliases are commonly used to display a meaningful or user-friendly name for a data value. For example, Financial Server might be defined as an alias for IP address 192.168.2.18. When selected, Guardium uses available aliases for all reports.
- PDF footer text: PDF files created by various Guardium components (such as audit tasks) have a standard page footer. To customize the footer, enter your text into the PDF footer text box. PDF footer text that you define on a central manager or aggregator is not distributed to managed units.

## Managing alert message templates

---

Message templates determine the content of alerts. You can create multiple message templates from the Global Profile, and use them with different rules as needed. Note: For more information about creating and managing message templates, see [The alert message template](#).

- Default message template: Displays the default message template for alerts.
- No wrap: Select to remove word wrap from the message template. Use this feature to see where the line breaks appear in the message.
- Named template: Click Edit to create new templates and manage or edit existing named templates. For more information, see [The alert message template](#).

## Specifying a CSV separator

---

Specify a CSV separator for all CSV output (such as audit processes):

- CSV separator: Select Comma, Semicolon, Tab, or click Other to define your own separator.

## Adding text to the Guardium window

---

- HTML - left and HTML - right: Enter HTML-formatted text to include at the bottom of the Guardium window.  
To verify that your HTML displays as you expect, click .
- Create a login message and other elements to display when (or before) a user logs in:
  - Show login message: Select to display the login message (or clear to disable the display).
  - Login message: Add a plain text message to display each time that a user logs in.
  - Pre-login message (HTML): Add an HTML-formatted message that displays after a user opens the Guardium window but before they log in.  
Note: If you include an image, the image also displays in the pre-login message. For more information, see [Upload logo image](#).
  - Header and footer banner (HTML): Add HTML-formatted banners to the Guardium login page. By default, the header and footer display at the top and the lower left of the Guardium UI. However, you can use HTML to change the alignment, color, and other elements for your requirements.

## Managing other Guardium properties

---

- Concurrent login from different IP: By default, the same Guardium user can log in to an appliance from multiple IP addresses. Use this feature to disable concurrent logins from the same user. When disabled, each user can log in from only one IP address at a time. If a user closes their browser without logging out, the connection times out due to inactivity, so the user account is not blocked for long.  
Note: When this feature is enabled, Unlock displays. For support purposes, you can unlock the account to allow a second user to log in with this user account from a different IP address.
  - Data level security filtering: Enable this feature when specific Guardium users are responsible for specific databases. Use data-level filtering to filter results system-wide so that each user can see only the information from databases for which that user is responsible.  
Note: If data level security at the observed data level is enabled, then audit process escalation is allowed only to users at a higher level in the user hierarchy.
  - Default Filtering: If data-level security filtering is enabled, you can set the default filtering options for the logged-in viewer.
    - Show all: The logged-in viewer can see all of the rows in the result regardless of who these rows belong to. When used with the datasec-exempt role, allows an override of the data level security filtering.
    - Include indirect records: The logged-in viewer can see the rows that belong to the logged-in user, and all rows that belong to users in the user hierarchy under the logged-in user.
- Note: The datasec-exempt role is activated when data level security is enabled and the datasec-exempt role is assigned to a user. For more information, see [Understanding Roles](#).
- Restriction: Data Level Security and the Investigation Dashboard cannot be enabled concurrently.
- Escalate result to all users: When enabled (the default), audit process results (and PDF versions) are escalated to all users, even if data level security at the observed data level is enabled. If not enabled, then audit process escalation is allowed only to users at a higher level in the user hierarchy and to users with the datasec-exempt role. If disabled (cleared), and no user hierarchy is available, then no escalation is allowed.
  - Custom database table maximum size (MB): Set the size of the custom database table (in MB). The Default value is 4000 MB. In addition, click Current Usage to display the current values for InnoDB, MyISAM, and the combined total.  
Note: The custom size limit is tested before data is imported. If a data import exceed the new limit, Guardium prevents the next import.
  - FTP/SCP Ports Export: Change a port to send files over FTP or Secure Copy Protocol (SCP). You can change the ports for export and patch backup. The default port for FTP is 21. The default port for SSH/SCP/SFTP is 22.  
Note: A zero indicates that Guardium uses the default port.
  - Encrypt Must Gather output: Guardium collects certain data (MustGather information) that IBM support uses if something goes wrong. Select to encrypt MustGather output. Clear to compress, but not encrypt the output.  
You can also turn MustGather encryption on and off from the CLI. For more information, see [store\\_encrypt\\_must\\_gather](#).
  - Check for Guardium updates: When selected, information about relevant ad hoc Guardium patches, GPUs, CFPs, bundles, Sniffer patches, and security patches display when you click the  icon.  
Note: After you install a patch, it is removed from the list.
  - Datasource connection timeout (seconds): Set the datasource connection timeout. The default is 60 seconds.

When you are done making changes, click Apply to save your changes to the global profile.

## Uploading a new logo

You can add or delete a graphic on the Guardium window.

- To delete the current logo, click Delete.
- To add a file, click Browse to select a file to upload to theGuardium appliance. Then, click Upload.
- When you refresh your browser window, the new image is scaled to 60 x 54 pixels and displays in the upper right corner of the Guardium UI. If you have a pre-login message, the image also displays in the message.

Note: The file name cannot include any of the following characters: Single quotation mark ('), double quotation mark ("), less than sign (<), or greater than sign (>).

## Managing access by IP address

From a central manager or stand-alone machine, use Manage login access by IP address to limit access to the Guardium UI, CLI (via SSH), or both to specified IP addresses.

To specify IP addresses for an allowlist:

1. From Manage login access by IP address, click Manage to open Manage login access by IP address.  
From here, you can either add IP addresses one at a time, or click Import from CSV to import a list of IP addresses from a comma-separated value (CSV) file.
2. To add a single IP address, click the  icon to open the Add IP address to allowlist window.
  - a. Enter the IP address (IPv4 or IPv6) you want to include.
  - b. Select the login type: GUI, SSH (to log in to the CLI), or GUI and SSH.
  - c. Click OK to add the address.
3. To import a list of address from a CSV file:
  - a. Click Browse and select a CSV file that contains the list of IP address to add to the allowlist.
  - b. If necessary, set Field delimiter to the separator used in the CSV file. The default is a comma (,).
  - c. Click Load to add the values.
  - d. Select the column within the file to import.
  - e. Select the login type: GUI, SSH (to log in to the CLI), or GUI and SSH.
  - f. Click OK to add the addresses.

Note: To include different addresses for the GUI and SSH allow lists, use separate CSV files.
4. The addresses that you added display in the IP address table. Select whether to enforce the allowlist for GUI or SSH logins, or both, and then click Save.

Users can now log in only if their IP addresses are in the allowlist.

To manage IP addresses in the allowlist:

- To disable the allowlist (that is, allow login access for any IP address), clear Enforce allowlist... for either GUI or SSH logins (or both).
- To remove addresses from the allowlist, select the addresses to delete and click the  icon.

Note: Be careful not disable access from your current IP address. If you do disable access, you (or someone with access to the GUI) can use the [update\\_ip\\_restriction\\_allowlist](#) API to restore access.

- [The alert message template](#)

Message templates determine the content of alerts. You can create multiple message templates from the Global Profile, and use them with different rules as required.

## The alert message template

Message templates determine the content of alerts. You can create multiple message templates from the Global Profile, and use them with different rules as required.

Several message templates available, which allow you to define the following types of messages:

- Threshold Alerts: Send an alert when Guardium detects that a specified threshold is met or exceeded.
- Audit Process Report: Publish in audit process reports.
- Real-time Alerts: Send an alert immediately when Guardium detects a problem.
- Audit Process Email: Sends an email when an audit process runs. You can customize the email as needed. For more information, see [Custom email template in Building audit processes](#).

You can use the filtering checkboxes to filter the types of templates to view.

Several predefined message templates are available for ArcSight, enVision, and IBM QRadar (in LEEF format) security information and event management (SIEM) solutions. Guardium® includes two certified (agreed upon) templates to integrate with these SIEM solutions.

## Creating or updating named messages

To add, modify, or delete named message templates:

1. Click Edit to open the Named Template Finder window.
2. Click to open the Modify Named Template window. The current default message template displays in the Default message template text box.  
Alternatively, select one of the existing named templates and click to clone that template. You can then rename and edit your new template.
3. Enter a name and template type for your new template. Then, add or delete the message template variables to meet your requirements. For more information about the available message template variables, see [Table 1](#).  
Select No wrap to see where the line breaks appear in the message.
4. Click Save when you are done.
5. Changes take effect after you restart the inspection engines from the managed unit.  
Note: To restart the inspection engines, browse to Manage > Activity Monitoring > Inspection Engines and then click Restart Inspection Engines.

## Formatting real-time alerts

Customizing email for real-time alerts

Use the **store alerter email append\_name\_subject** and **store alerter email append\_subject\_body** CLI commands to customize emails from real-time alerts as follows:

- Control the appearance of the Prefix email subject with Guardium appliance name.
- Control the appearance of the email subject in the email body.
- Add naming template parameter %%applianceHostName to add the appliance hostname to Name Templates (in either the subject or the body).

Setting sender encoding

To encode outgoing messages (email and SNMP traps) in an encoding scheme other than UTF8, use the **store sender\_encoding** CLI command, as described in [store sender\\_encoding](#).

## Alert message template variables

Table 1. Alert message template variables.

Note: Only the following variables in the Alert template are available for correlation alerts.

- Subject: %%Subject[Guardium Alert. Severity: (%severity), Alert Name: %%alertName]  
Alert Name: %%alertName  
Alert Description: %%description  
Current value: %%alertQueryValue  
Base query value: %%alertBaseQueryValue  
Threshold: %%alertThreshold
- Query period: %%alertQueryFromDate - %%alertQueryToDate  
Alert Classification: %%classification  
Category: %%category  
Severity: %%severity
- Recommended Action: %%recommendation

| Variable | Description |
|----------|-------------|
|----------|-------------|

| Variable               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| %%analyzedClientIP     | A client IP field populated by the Guardium Analyzer. Corresponds to GDM_ACCESS.ANALYZED_CLIENT_IP. If the Analyzed Client IP is not available when the SQL event is processed: <ul style="list-style-type: none"> <li>If the policy rule action is set to Alert only and SYSLOG notification, then %%analyzedClientIp is blank.</li> <li>A value for analyzedClientIp is not always available for encrypted Oracle traffic.</li> <li>For any other alert policy rule actions, the alert message might be delayed and sent later in the session.</li> </ul>                                                                                                                           |
| %%AppEventType         | The type of application event.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| %%AppUserName          | Application username.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| %%AuthorizationCode    | Authorization code.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| %%BindVarVal           | Available for Db2 z/OS systems only. The bind variable value, which is replaced with the values from the "FULL SQL"."Bind Variables Values" in the FULL SQL entity. For more information, see the <a href="#">Attributes for Full SQL Entity (Db2 for z/OS) table</a> .                                                                                                                                                                                                                                                                                                                                                                                                               |
| %%category             | Category from the rule definition.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| %%CICSUser             | Available for Db2 z/OS systems only. %%CICSUser is either: <ul style="list-style-type: none"> <li>The CICSEndUser.</li> <li>The CICS user ID (same as %%EndUser), if the sysConType is CICS (value of 4).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| %%classification       | Classification from the rule definition.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| %%ClientAcctn          | Available for Db2 z/OS systems only. Contains information from the Db2 z/OS CURRENT CLIENT_ACCTNG special register. For more information, see the Special registers documentation for your version of Db2 for z/OS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| %%ClientApplnName      | Available for Db2 z/OS systems only. Contains information from the Db2 z/OS CURRENT CLIENT_APPLNAME special register. For more information, see the Special registers documentation for your version of Db2 for z/OS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| %%clientHostname       | Client hostname.<br>For Db2 z/OS users: If the <b>store snif_db2z_alert_use_client_ip_for_host_name</b> CLI command is set to <i>on</i> , then %%clientHostname stores the client IP address. For more information, see <a href="#">store snif_db2z_alert_use_client_ip_for_host_name</a> .                                                                                                                                                                                                                                                                                                                                                                                           |
| %%clientIP             | Client IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| %%clientPort           | Client port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| %%ClientWrkstn         | Available for Db2 z/OS systems only. Contains information from the Db2 z/OS CURRENT CLIENT_WRKSTNNNAME special register. For more information, see the Special registers documentation for your version of Db2 for z/OS.                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| %%compressed_uid_chain | For Linux or UNIX systems only, the compressed UID chain that tracks a chain of users.<br>Messages that include this variable are delayed for 5 minutes by default. For more information, see the <a href="#">store alerter delay</a> CLI command. The value is then replaced with the "Session"."Uid Chain Compressed" values from Guardium report attributes. For more information, see <a href="#">UID chains</a> .<br><br>Note: This variable does not return a value when used with a message template, which uses an <i>alert only</i> policy rule action that specifies the <i>syslog</i> notification type. For more information, see <a href="#">Alerting rule actions</a> . |
| %%ConstructID          | Construct ID in the SQL request associated with the alert message.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| %%CurrentDBUser        | Available for Db2 for IBM® i only. %%CurrentDBUser is the name of the current Db2 for i user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| %%DBName               | Database name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| %%DBProtocol           | Database protocol.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| %%DBProtocolVersion    | Database protocol version.<br>For Db2 z/OS users: %%DBProtocolVersion is populated only if your S-TAP version supports the DB Protocol Version parameter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| %%DBUser               | Database username.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| %%EndUser              | Available for Db2 z/OS systems only. %%EndUser is either: <ul style="list-style-type: none"> <li>The Db2 application user.</li> <li>The CICS user ID, if the z/OS Collector Agent is configured to collect the CICSUserID.</li> </ul> For other databases, %%EndUser is blank.                                                                                                                                                                                                                                                                                                                                                                                                        |
| %%EventDate            | The date of the App Event.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| %%EventValueNum        | The App Event value number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| %%EventValueStr        | The App Event value string.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| %%IMSPartArea          | Available for IMS only. Corresponds to "FULL SQL"."IMS PART/AREA". Can be either a HALDB partition name or a DEDB AREA name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| %%lastError            | Last error description: Available only when an SQL error request that triggers an exception rule contains a last error description field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| %%netProtocol          | Network protocol, for K-TAP on Oracle, which can display as either IPC or BEQ.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| %%Object               | A list of objects matching the rule. List the number of objects is based on the value of the <a href="#">store alert_object_num_limit</a> CLI command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| %%objectType           | The type of each object returned by the list of objects in %%Object.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| %%OSUser               | Session information. (OS_USER in GDM_ACCESS).<br>For IMS z/OS systems, the %%OSUser is the same as the %%DBUser.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| %%Program              | Available for Db2 for IBM® i only. The program schema/program.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| %%ProcessID            | Available for Db2 for IBM® i only. The job number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| %%receiptTime          | Timestamp representing the time when the alert occurred. %%receiptTime displays in either seconds or milliseconds, based on the value of the <a href="#">store alert_timestamp_unit</a> CLI command. The default is seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| %%receiptTimeMills     | Number representing the time when the alert occurred, in milliseconds, since the fixed date of Jan 1 1900.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Variable            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| %%RecordsAffected   | Records affected.<br>Messages that include this variable are delayed for 5 minutes by default. For more information, see the <a href="#">store alerter delay</a> CLI command.<br><br>Note: This variable does not return a value when used with a message template, which uses an <i>alert only</i> policy rule action that specifies the <i>syslog</i> notification type. For more information, see <a href="#">Alerting rule actions</a> .                                                                                                                                                                                                                   |
| %%requestType       | Request type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| %%ResponseLength    | Response length. Not supported for Db2 z/OS systems.<br>Messages that include this variable are delayed for 5 minutes by default. For more information, see the <a href="#">store alerter delay</a> CLI command.<br><br>Note: This variable does not return a value when used with a message template, which uses an <i>alert only</i> policy rule action that specifies the <i>syslog</i> notification type. For more information, see <a href="#">Alerting rule actions</a> .                                                                                                                                                                                |
| %%ReturnedDataCount | The returned data count for extrusion rules. Requires that the Inspect Returned Data flag is on.<br>Note: This variable does not return a value when used with a message template, which uses an <i>Alert only</i> policy rule action for access rules.                                                                                                                                                                                                                                                                                                                                                                                                        |
| %%ruleDescription   | The rule description from the policy rule definition.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| %%ruleID            | The rule number from the rule definition.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| %%SenderIP          | The IP address of the server where the S-TAP is installed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| %%serverHostname    | Server hostname.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| %%serverIP          | Server IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| %%serverPort        | Server port number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| %%serverType        | The database server type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| %%serviceName       | Service name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| %%SessionID         | Session ID. The Session_id is the same as the MySQL auto-generated ID in GDM_SESSION on the collector.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| %%sessionStart      | Session start time (login time).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| %%sessionStartMills | Number representing the start of the session where the alert occurred, in milliseconds since the fixed date of Jan 1 1900.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| %%severity          | Severity from the rule definition.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| %%SourceProgram     | Source program name. For Db2 for IBM i, the %%SourceProgram returns job_user/job_name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| %%SQLNoValue        | SQL string with masked values. The value of SQL is replaced by a question mark (?) in the syslog.<br>For IMS z/OS users: The following values are available, similar to the %%SQLString values: prog=; job=; step=; tran=; job#=.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| %%SQLString         | SQL string (if any).<br>Note: For databases that generate custom queries, %%SQLString values are copied to %%SQLNoValue, where they are masked. These databases include, for Cloudera: HDFS, HBASE, and SOLR; for Hortonworks: HBASE, HDFS, KAFKA, SOLR, STORM, and YARN.                                                                                                                                                                                                                                                                                                                                                                                      |
| %%SQLTimestamp      | The time on the packet or request. %%SQLTimestamp displays in either seconds or milliseconds, based on the value of the alert_timestamp_unit CLI. The default is seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| %%Subject[ ]        | If you specify this variable, all of the text between the square brackets ([ ]), such as file name, email sender, or description, is included in the subject line of the email that is sent to the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| %%succeeded         | Messages that include this variable are delayed for 5 minutes by default. For more information, see the <a href="#">store alerter delay</a> CLI command. The value is replaced with the "FULL SQL"."Succeeded" value from Guardium report attributes.<br>Note: This variable does not return a value when used with a message template, which uses an <i>alert only</i> policy rule action that specifies the <i>syslog</i> notification type. For more information, see <a href="#">Alerting rule actions</a> .                                                                                                                                               |
| %%uid_chain         | For Linux or UNIX systems only, the UID chain that tracks a chain of users.<br>Messages that include this variable are delayed for 5 minutes by default. For more information, see the <a href="#">store alerter delay</a> CLI command. The value is then replaced with the "Session"."Uid Chain" value from Guardium report attributes. For more information, see <a href="#">UID chains</a> .<br><br>Note: This variable does not return a value when used with a message template, which uses an <i>alert only</i> policy rule action that specifies the <i>syslog</i> notification type. For more information, see <a href="#">Alerting rule actions</a> . |
| %%UnitOfWork        | Computed attribute that contains the CICS Unit of Work ID in hex to correlate CICS traffic across multiple S-TAP Entities (IMS, data sets, and Db2).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| %%Verb              | The SQL verbs that are relevant to the triggered rules in the alert messages. You can set the number of SQL verbs to include by setting the ALERT_VERB_NUM_LIMIT parameter from the <a href="#">modify_guard_param</a> command. The default is 10. For more information, see <a href="#">Alerter parameters</a>                                                                                                                                                                                                                                                                                                                                                |
| %%violationID       | Numeric representing the POLICY_VIOLATION_LOG_ID of this alert in GDM_POLICY_VIOLATION_LOG (this is the same as the Violation Log ID in the Policy Violations / Incident Management report).                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## Example: Creating a real-time alert

The following example shows the general process of creating a Guardium real-time alert. Your process might be different.

1. Create a message template for your alert:
  - a. From the Named Template Finder in the Global Profile UI, select and clone a real-time alert template. You can use the filtering to select the template type that you want.
  - b. Name your new template and click Save to save it.
  - c. From the Named Template Finder, select your new template and click to make changes. Add or remove the message template variables (described in [Table 1](#)) as needed, and then save the changes.
2. Associate your alert with a policy:
  - a. Open Security Policies (Policy Builder for Data) and select or create a policy.
  - b. Create a rule for your policy (for example, a session level rule of *Database type = ORACLE*).
  - c. Under Rule action, add an action and specify your template as the Message Template.
  - d. Click OK to save the new Action, OK again to save the rule, and OK one more time to save the policy.
3. From the Guardium Alerter page, make sure that the alerter is running.
4. The next time Guardium starts, if Guardium fires the alert, a message is sent to the SYSLOG that contains the information that is specified in your alert message.

## Configuring the alerter

Configure and activate the alerter to send email messages, SNMP traps, and alert-related Syslog messages.

Other components create and queue messages for the Alerter. The Alerter checks for and sends messages based on the specified polling interval.

To configure, enable or disable individual correlation alerts, see [Correlation Alerts](#). To produce correlation alerts and appliance alerts, make sure that Anomaly Detection is started. To create real-time alerts, a security policy must be installed.

Mail/SNMP/SYSLOG messages are sent out according to their priority.

To open the Alerter page, go to Setup > Tools and Views > Alerter.

### Automatically activate the Alerter on startup

1. Select Active on Startup. Each time the appliance restarts, the Alerter is activated.
2. Click Apply.
3. If the Alerter is not running, click Restart to start it.

### Set the polling interval

The polling interval is the frequency that the Alerter checks for and sends messages. Enter the polling interval, in seconds.

### Configure the Alerter to send SMTP (email) messages

From the SMTP tab, configure email messages.

1. To use SMTP for alert emails, select Send alert emails using SMTP.
  2. Host, enter the IP address or hostname for the SMTP gateway.
  3. Under Port, enter the SMTP port number (the default is 25).
  4. If you selected Send alert emails using SMTP, click Test Connection to open the Test connection window. You can take one of the following actions:
    - Enter an email address to send the test alert and click OK to send a test email to the address.
    - Click OK without entering an address to test whether the connection is open (and return a message).
    - Click Cancel to cancel without testing.
  5. In Return-path email address, enter the return address for email that is sent by the system. This address is usually a monitored administrative account.
  6. Select Use STARTTLS for encryption to use STARTTLS to encrypt mail messages with TLS encryption.
  7. To use SMTP server authentication, select Assign SMTP credentials. In this case, you must specify the username and password to use for authentication.
    - Enter a valid username for your mail server.
    - Enter, and then reenter, the password for this user.
  8. Click Save to save the configuration.
- Note: The Alerter does not use the new configuration until it is restarted.
9. Click Restart to restart the Alerter with the new configuration.

### Configure the alerter to use SNMP

From the SNMP tab, you can configure SNMP traps for either SNMP v2c or v3.

To use SNMP for alert emails, select Send alert emails using SNMP and then select the SNMP version.

- For SNMP v2c, provide the following information:
    1. Under Primary host, enter the IP address or hostname to which to send the SNMP trap.
    2. Optionally, click Test Connection to verify the SNMP address and port (162). This only tests that access is available to specified host and port. The test does not verify that it is a working SNMP server. A dialog box displays that informs you of the success or failure of the operation.
    3. Under Trap community name and Re-enter trap community name, enter the community name for the trap.
    4. Optionally, select Secondary host to enable the ability to add a secondary host:
      - a. Under Secondary host, enter the IP address or hostname to which to send the SNMP trap.
      - b. Optionally, click Test Connection to verify the SNMP address and port.
      - c. Under Trap community name and Re-enter trap community name, enter the community name for the trap.
  - For SNMP v3, provide the following information:
    1. Under Primary host, enter the IP address or hostname to which to send the SNMP trap.
    2. Optionally, click Test Connection to verify the SNMP address and port (162). This only tests that access is available to specified host and port. The test does not verify that it is a working SNMP server. A dialog box displays that informs you if the operation was successful or failed.
    3. Under User name, provide the name of the SNMP user.
    4. Under Authentication protocol, select either the MD5 or SHA protocol. The default is MD5.
    5. Enter (and then re-enter) an authentication password.
    6. Under Encryption protocol, select either AES or DES encryption. The default is AES.
    7. Enter (and then re-enter) an encryption password.
  - Click Save to save the configuration.
- Note: The Alerter does not use the new configuration until it is restarted.
- Click Restart to restart the Alerter with the new configuration.

### Set up the external ticketing system

From the Alerter page, you can go to the External Ticketing System page to set up external tickets for alerts. For more information, see [Configuring an external ticketing system](#).

## Related concepts

---

- [The alert message template](#)
- 

## Facility and priority of syslog messages

---

The facility and priority of messages configured in the Guardium syslog can impact how they are consumed by the Security Incident Event Manager (SIEM).

You can send a few types of messages to the syslog:

- Policy Alerts. For more information, see [How to create a real-time alert](#).
- Correlation Alerts. For more information, see [Correlation alerts](#).
- Audit Process results. For more information, see [Building Audit Processes](#).
- Guardium® predefined alerts. See [Predefined alerts](#).

## Policy alerts and correlation alerts

---

When defining a policy or correlation alert, there are five levels of severity that can be picked from the drop down list:

- info
- low
- none
- med
- high

The syslog messages are assigned a specific facility and priority for each configuration of severity:

| Severity of Policy Rule | Facility | Priority |
|-------------------------|----------|----------|
| info                    | daemon   | info     |
| low                     | daemon   | warning  |
| none                    | daemon   | warning  |
| med                     | daemon   | error    |
| high                    | daemon   | alert    |

## Audit Process results

---

The Audit Process results are assigned the following facility and priority:

| Severity of Policy Rule | Facility | Priority |
|-------------------------|----------|----------|
| NA                      | user     | info     |

## Anomaly Detection

---

The Anomaly Detection process runs every polling interval to create and save, but not send, correlation alert notifications that are based on an alert's query.

This notification is run according to the schedule defined for each alert. See [Configuring the alerter](#) for more information about sending notifications.

The Anomaly Detection process uses the results of a correlation alert's query, which looks back over a specified period of time, and the correlation alert's threshold, to determine whether a condition is satisfied (an excessive number of failed logins, for example). See [Correlation Alerts](#) for more information.

In a Central Manager environment, the Anomaly Detection panel for each Guardium system can be used to turn off correlation alerts that are not appropriate for that particular Guardium system. Under Central Management, all correlation alerts are defined on the Central Manager, regardless of which Guardium system they were created or updated. These correlation alerts are the same for all Guardium system, and when activated, are activated on all Guardium system by default.

Note: The Alerter component must be configured and started to send a saved alert message to SYSLOG, email, or an SNMP trap.

Note: Anomaly Detection does not play a role in the production of real-time alerts, which are produced by security policies.

## Automatically activate Anomaly Detection on startup

---

1. Click Setup > Tools and Views > Anomaly Detection to open Anomaly Detection.
2. Mark the Active on Startup check box. Each time the Guardium system restarts, Anomaly Detection is activated automatically.
3. Click Apply.

## Set the frequency that Anomaly Detection checks for appliance issues

---

1. Click Setup > Tools and Views > Anomaly Detection to open Anomaly Detection.
2. Enter the Polling Interval in minutes.
3. Click Apply.

## Enable or Disable Active Alerts

---

To disable an alert globally in a central manager environment, use the alert builder: navigate to Protect > Database Intrusion Detection > Alert Builder and clear the Active check box in the Modify Alert panel.

To enable or disable an alert on a single Guardium system in a central management environment, follow these steps:

1. Log in to the UI of the Guardium system on which you want to disable one or more alerts.
2. Click Setup > Tools and Views > Anomaly Detection to open Anomaly Detection.
3. To disable an alert, select it from the Active Alerts box, and click Disable.
4. To enable an alert, select it from the Locally Disabled Alerts box, and click Enable.

## Stop or Restart Anomaly Detection

---

1. Click Setup > Tools and Views > Anomaly Detection to open Anomaly Detection.
  2. Click Stop to stop Anomaly Detection, or click Restart to restart it.
- 

## Session Inference

Session Inference checks for open sessions that have not been active for a specified period of time, and marks them as closed.

To configure the Session Inference options:

1. Click Setup > Session Inference to open Session Inference.
2. Mark the Active On Startup box to start Session Inference on startup of the Guardium® system.
3. In the Polling Interval box, enter the frequency (in minutes) with which Session Inference checks for open sessions. The default is 120 (minutes).
4. In the Max Inactive Period box, enter the number of minutes of inactivity after which a session is marked closed. The default is 720 (minutes).
5. Click Apply to store the values in the configuration database. Session Inference will not begin using a new configuration until it is restarted.
6. Click Restart to restart Session Inference with the new configuration.

To stop Session Inference, open the Session Inference panel and click Stop.

---

## Allow (approve) S-TAP connection to Guardium (S-TAP certification)

Use this function to control the specific S-TAP hosts whose clients are allowed ("approved") to access the Guardium® system.

### About this task

---

When enabled, only the specified S-TAP clients are allowed to access the Guardium system.

You can also control this feature with the CLI command **store\_stap\_approval** or with the GuardAPI command, **grdapic store\_stap\_approval**.

If you use the CLI command **store\_stap\_approval**, the new configuration takes effect after you run the command **restart inspection-core**.

View approved S-TAPs in Manage > Reports > Change Monitoring > Approved Tap Clients or Reports > Real-Time Guardium Operational Reports > Approved Tap Clients.

### Procedure

---

1. Access Manage > Activity Monitoring > S-TAP Certification.
2. Select S-TAP Approval Needed. This is the equivalent of the GrdAPI command **store\_stap\_approval**.
3. Specify the approved S-TAP host IP address (not host name) in the Approved S-TAP Clients section, and click Add. This is the equivalent of the GrdAPI command **add\_approved\_stap\_client**.
4. Repeat for each S-TAP host.

### Results

---

Note: In a Central Managed environment, after you add the IP addresses to approved S-TAPs, there is a wait time for synchronization that might take up to an hour. After synchronization is complete, the status of the approved S-TAPs appears green in Manage > Activity Monitoring > S-TAP Control.

### Related reference

---

- [store\\_stap\\_approval](#)
  - [add\\_approved\\_stap\\_client](#)
- 

## IP to Hostname Aliasing

The IP-to-Hostname Aliasing function accesses the Domain Name System (DNS) server to define hostname aliases for client and server IP addresses.

There are two separate sets of IP addresses: one for clients, and one for servers. When IP-to-Hostname Aliasing is enabled, alias names will replace IP addresses within Guardium® where appropriate.

1. Click Protect > Database Intrusion Detection > IP-to-Hostname Aliasing to open IP-to-Hostname Aliasing.
2. Mark the check box for Generate Hostname Aliases for Client and Server IPs (when available) to enable hostname aliasing.

A second check box can now be accessed. The name of this check box is Update existing Hostname Aliases if rediscovered.

3. Mark the check box to update a previously defined alias that does not match the current DNS hostname (usually indicating that the hostname for that IP address has changed). You may not want to do this if you have assigned some aliases manually. For example, assume that the DNS hostname for a given IP address is dbserver204.guardium.com, but that server is commonly known as the QA Sybase Server. If QA Sybase Server has been defined manually as an alias for that IP address, and the check box for Update existing Hostname Aliases if rediscovered is marked, that alias will be overwritten by the DNS hostname.
4. Click Apply to save the IP-to-Hostname Aliasing configuration.
5. Do one of the following:
  - Click Run Once Now to generate the aliases immediately.
  - Click Define Schedule to define a schedule for running this task. See [Scheduling](#) for more information.

To view the aliases defined, see [Aliases](#).

## Configure Permission to Socket connection

This topic applies to Custom Alerting Classes.

Follow this procedure to configure permissions for socket all connections that are used by custom classes.

1. Click Setup > Evaluations > Communication Permissions to open the Communication Permissions.
2. Click Add permission To Socket Connection to expand that pane.
3. Enter the IP address or Host name for the host.
4. Enter a Port number for the socket connection.
5. Enter a description.
6. Click Save.

## Managing access to Guardium

Access management consists of four tasks: account administration, maintenance, monitoring, and revocation.

Access Management is separate from system administration duties.

There are two predefined users on a Guardium® appliance: accessmgr and admin.

- *accessmgr* is the user name assigned to the access manager. By default, the access manager is the only user authorized to manage user accounts and security roles.
- *admin* is the user name assigned to the (primary) Guardium administrator. By default, the administrator does not have authority to manage user accounts or security roles. The admin user has a more extensive set of privileges.

Note: Admin and accessmgr roles can not be assigned to the same user. The same user may contain both of these roles through a legacy situation or as a result of an upgrade. However, current use will not allow the two roles to be assigned to the same user.

## Access Management Selection

- User Browser: Manage users
- Role Browser: Manage permissions and customize layouts for roles
- Role Permissions: Manage application permissions
- LDAP User Import: Import users from LDAP

## Data Security Selection

- Datasources Associated
- Datasources Not Associated
- Servers Associated
- Servers Not Associated
- User Hierarchy
- User-DB Association

## Predefined Reports from Accessmgr

The following predefined reports are available from the Accessmgr user.

## User and Role Reports

Defining and modifying users (see [Managing users](#)) involves deciding both who will be using the Guardium system and to what roles (see [Understanding Roles](#)) they will be assigned. A role is a group of users, all of whom are granted the same access privileges.

The User and Role Reports consist of reports:

- User - Role: a report that shows, by user, the number of roles that user belongs to.
- All Roles - User: a report that shows, by role, the number of users that belong to that role.

Note: admin and access manager are pre-existing, other roles are created by the Access manager.

The following reports are available on a Central Manager or a standalone unit. If trying to use on a managed machine, an error message will appear. Servers Not Associated will show servers from ALL managed units in Central Manager systems.

## Datasources Associated

---

This report identifies Datasource Name, Host, Service Name, Login Name and Association Type. This information comes from the choices made in the User-Database Associations activity. See the Data User Security - Hierarchy and Associations help topic.

## Datasources Not Associated

---

This report is a list of datasources not associated with any users. This report identifies Datasource Name, Datasource Type, Host, and Service Name. This information comes from the choices made in the User-Database Associations activity. See the Data User Security - Hierarchy and Associations help topic.

## Servers Associated

---

This report identifies Server IP, Service Name, Login Name and Association Type. This information comes from the choices made in the User-Database Associations activity. See the Data User Security - Hierarchy and Associations help topic.

## Servers Not Associated

---

This report is a list of servers not associated with any users. This report identifies Server IP and Service Name. This information comes from the choices made in the User-Database Associations activity. See the Data User Security - Hierarchy and Associations help topic.

- [Understanding Roles](#)

Assign a role to a Guardium user to grant them specific access privileges. Some examples of roles are: CLI, admin, accessmgr, CAS, and user.

- [Access for default roles and applications](#)

This topic lists user interfaces and other tools associated with the default roles and applications used for access management.

- [Managing roles and permissions](#)

Roles and permissions provide different levels of access to users based on their job duties.

- [How to create a role with minimal access](#)

This topic explains how to create a new role with minimal access permissions, for example an auditor role that can only access the Audit Process To-Do List and view specific reports.

- [Managing users](#)

Use the Access Manager, assigned the username accessmgr to add user accounts, enable or disable user accounts, import members from LDAP, or edit user permissions. Open the User Browser and browse the user accounts by clicking Access > Access Management > User Browser

- [Managing Guardium credentials with CyberArk](#)

You can use CyberArk to manage your Guardium credentials. For more information on this application, access the CyberArk Marketplace web page and search for Guardium.

- [Creating a user who can run GuardAPI commands](#)

Create a user who has the proper roles and entitlements to run GuardAPI commands from the command-line interface (CLI).

- [Importing users from LDAP](#)

You can import Guardium user definitions from one or more LDAP servers by configuring an operation that imports the set of users who need Guardium access.

- [Data Security - User Hierarchy and Database Associations](#)

You can use data security features to create a hierarchy of users and associate users to specific databases and servers. Guardium data security features report on which users accessed what information, and ensure that only specific users see information that they are responsible for.

- [How to define User Hierarchies](#)

Use the UI from an access manager account to easily define user hierarchies.

---

## Understanding Roles

Assign a role to a Guardium user to grant them specific access privileges. Some examples of roles are: CLI, admin, accessmgr, CAS, and user.

The access manager defines roles and assigns them to users and applications. When a role is assigned to an application or the definition of an item (a specific query, for example), only those Guardium users who are also assigned that role can access that component.

When user definitions are imported from an LDAP server, the groups to which they belong can optionally be defined as roles. For more information, see [Importing users from LDAP](#).

Note: When assigning roles to a user, the admin and access manager role cannot be assigned to the same user.

Note: Custom-created roles cannot be combined with default-provided roles (examples are user, admin, accessmgr, cli, inv, datasec-exempt, review-only).

Note: Admin role and object owner have access to all objects by default.

Note: Taking a base role and customizing (with additional navigation items), and then copying this customized role, will result in a loss of the customization if the customized or copied role is reset to default.

---

## Default Roles

The Guardium system is pre-configured to support users who fall into four broadly defined default roles: admin, user, access manager, and investigations. The Guardium access manager can create new roles as well.

Note: Note: If data level security at the observed data level is enabled (see Global Profile settings), then audit process escalation is allowed only to users at a higher level in the Data Hierarchy (see Access Manager). The Datasec-exempt user can escalate, without restrictions, to anyone.

Table 1. Default Roles

| Default Role | Description                                                                                |
|--------------|--------------------------------------------------------------------------------------------|
| user         | Provides the default layout and access for all common users. This role can not be deleted. |

| Default Role   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| admin          | Provides the default layout and access for Guardium administrators. Do not confuse the admin role with the admin user, which is a special user account having the admin role, but also having additional powers that are reserved for the admin user account only. This role can not be deleted.                                                                                                                                                                                                                                                                                                         |
| accessmgr      | Provides the default layout and access for the access manager. This role can not be deleted.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| cli            | Provides access to CLI. The admin user has default access to CLI. Everyone else must be given permission when users are created by access manager and roles specified. The access manager can define as many users in the system and give them the CLI role. These users have access to the CLI and all activities of their CLI sessions are associated with this user.<br><br>To run GrdAPI or CLI commands without admin rights, click the role CLI for Admin Console in the User Role Permissions selection.<br><br>See the topic, <a href="#">diag CLI Command</a> , on how to manage the diag role. |
| inv            | Provides the default layout and access for investigation users. An investigation user must have the restore-to database name of INV_1, INV_2 or INV_3, as the Last Name in their user definition. This is not enforced by the GUI, but is required for the application to function properly. When assigned, the user role must also be assigned. This role can not be deleted.<br><br>Note: The Ad-Hoc Process for run once now button is available on all report screens for all users except investigation (INV) user.                                                                                 |
| datasec-exempt | Data Security - Exempt. This role is activated when Data level security is enabled (see Global Profile in Administration Console) and the datasec-exempt role has been assigned. If the user has this role, a Show all check box appears in all reports. If checked, all sniffed data records are shown (no filter is applied). This role cannot be deleted in the Role Browser.                                                                                                                                                                                                                         |
| review-only    | A user that is specified by this role can view only results (Audit, Assessment, Classifier), Audit Results and the To Do List. This role cannot be deleted in the Role Browser.<br><br>Users with this role is allowed to enter comments in the audit process viewer (not workflow or comments/data per row, but comments at process/result level).<br><br>Users with this role cannot perform any changes/actions on any workflow automation result (escalate, reassign, etc).                                                                                                                          |

## Sample Roles

In addition to the default roles, a set of sample roles is also defined.

Table 2. Sample Roles

| Sample Role           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dba                   | Users who have a database-centric view of security, allowing access to database-related reports and tracking of database objects                                                                                                                                                                                                                                                                                                                                                                                                                          |
| infosec               | Users who have an information security focus, including tracking access to the database, and handling network requests, audits, and forensics                                                                                                                                                                                                                                                                                                                                                                                                             |
| netadm                | Users who have a network-centric view, including IP sources for database requests                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| appdev                | Application developers, architects, and QA personnel who have an application-centric focus and want to track and report on SQL streams generated by an application                                                                                                                                                                                                                                                                                                                                                                                        |
| audit                 | Auditors and others who need to view audit reports<br><br>Note: If trying to copy this role, an embedded message will appear explaining that not all aspects of this role can be copied. The message is: "Create a new role using the layout and permission from the "audit" role. Special privileges and actions associated with the "audit" role will not be copied."                                                                                                                                                                                   |
| audit-delete          | This role is used to track or log when an audit process result has been deleted. Users with the audit-delete role can delete reports. Admin users can also delete reports. Tracking is done through the User Activity Audit Trail report.                                                                                                                                                                                                                                                                                                                 |
| admin-console-only    | A user that is specified by this role can only access the admin console tab.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| cas                   | Configuration Auditing System (CAS)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| vulnerability-assess  | A user that is specified by this role can view only vulnerability results.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| diag                  | A user that is specified by this role can access and run the diag commands in CLI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| workload-replay-admin | A user that is specified by this role can define and modify the workload-replay functions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| workload-replay-user  | A user that is specified by this role can run the workload-replay functions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| tam                   | A user that is specified by this role can define and modify the File Activity Monitor functions.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| BaselII               | Accelerator - Basel II. This role can not be deleted.<br><br>Basel II Part 2 Sections 4 and 5 require that banking institutions must define a Securitization Framework around financial information and estimate the associated operational risk.                                                                                                                                                                                                                                                                                                         |
| DataPrivacy           | Accelerator - DataPrivacy. This role can not be deleted.<br><br>The Data Privacy Accelerator delivers a portfolio of pre-configured policies, real-time alerts, and audit reports that are specifically tailored to the challenges of identify theft and based on industry best practices. With the Data Privacy Accelerator, security managers, privacy officers, and database administrators begin by defining combinations of data elements – called "privacy sets" – whose access may indicate hacking or inappropriate activities by internal users. |
| GDPR                  | Accelerator - GDPR. This role can not be deleted.<br><br>The Guardium GDPR accelerator provides the GDPR workflow for data ,and predefined reports based on GDPR groups and policies. To begin working with the GDPR accelerator, assign the GDPR role to a Guardium user, then navigate to Accelerators > GDPR with that user account.                                                                                                                                                                                                                   |
| GDPR FAM              | Accelerator - GDPR FAM. This role can not be deleted.<br><br>The Guardium GDPR FAM accelerator provides the GDPR workflow for file servers, and predefined reports based on GDPR groups and policies. To begin working with the GDPR FAM accelerator, assign the GDPR FAM role to a Guardium user, then navigate to Accelerators > GDPR with that user account.                                                                                                                                                                                           |

| Sample Role | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pci         | Accelerator - PCI. This role can not be deleted.<br>The PCI DSS is a set of technical and operational requirements designed to protect cardholder data and applies to all organizations who store, process, use, or transmit cardholder data. Failure to comply can mean loss of privileges, stiff fines, and, in the case of a data breach, severe loss of consumer confidence in your brand or services. The IBM® Guardium accelerator helps guide you through the process of complying with parts of the standard using predefined policies, reports, group definitions, and more. |
| sox         | Accelerator - SOX. This role can not be deleted.<br>SOX Section 404 requires that companies must establish and maintain an adequate internal control structure and procedures for financial reporting.                                                                                                                                                                                                                                                                                                                                                                                |

## Roles in a Central Manager Environment

In Central Manager environments, all User Accounts, Roles, and Permissions are controlled by the Central Manager. To administer any of these definitions, you must be logged in to the Central Manager (and not to a managed unit).

### Create a Role

1. Login as accessmgr, and open the User Role Browser by clicking Access > Access Management > Role Browser.
2. Click Add Role to open the Role Form panel.
3. Enter a unique name for Role Name and click Add Role.

### Remove a Role

1. Open the User Role Browser by clicking Access > Access Management > Role Browser.
2. Click Delete for any role (some roles cannot be removed, and do not have the Delete option). This opens the Role Form for the role.
3. Click Confirm Deletion. A message displays informing you that all references to the role are removed, and you will be asked to confirm the action.
4. Click OK to confirm the deletion, or Cancel to abort the operation.

## Access for default roles and applications

This topic lists user interfaces and other tools associated with the default roles and applications used for access management.

Use this information for auditing the Guardium functionality users can access when they are assigned specific roles.

Important:

- Not all functionality is available on all systems. The specific functions available on a system are determined by several factors including the Guardium version, the system configuration (standalone, central manager, etc.), and the installed licenses.
- Not all accessible user interfaces are displayed in the navigation by default, but a user can configure their navigation to display any user interface that is accessible to their roles. For more information, see [Customizing the user interface](#).

| Access management application             | Default Roles | Access                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Active Threat Analytics                   | user, admin   | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Manage &gt; Maintenance &gt; Active Threat Analytics Setup (admin role only)</li> <li>• Protect &gt; Uncover Threat Vectors &gt; Active Risk Spotter</li> <li>• Protect &gt; Uncover Threat Vectors &gt; Active Threat Analytics</li> </ul> |
| Alert Builder                             | ALL           | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Protect &gt; Database Intrusion Detection &gt; Alert Builder</li> <li>• Setup &gt; Tools and Views &gt; Alias Builder</li> <li>• Accelerators &gt; Data Privacy &gt; Tools &gt; Alias Builder</li> </ul>                                    |
| Allow Full SQL Drill Down                 | All           | Allows access to the Show SQL with Values menu option in reports.                                                                                                                                                                                                                                                                    |
| Analytic                                  | admin         | Controls access to the "Analytic Outliers Summary," "Analytic Outliers Details," "Analytic User Feedback," and "Analytic Outliers Status" domains.                                                                                                                                                                                   |
| Analyze DB                                | admin         | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Manage &gt; Maintenance &gt; Analyze System Database</li> </ul>                                                                                                                                                                             |
| Application User Responsibility Detection | admin         | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Protect &gt; Database Intrusion Detection &gt; Application User Translation</li> <li>• Protect &gt; Database Intrusion Detection &gt; Custom ID Procedures</li> </ul>                                                                       |
| Audit Database Builder                    | admin         | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Harden &gt; Configuration Change Control (CAS Application) &gt; Value Change Audit Database Creation</li> <li>• Harden &gt; Configuration Change Control (CAS Application) &gt; Value Change Audit Database Update &amp; Upload</li> </ul>  |

| <b>Access management application</b> | <b>Default Roles</b>                            | <b>Access</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Audit Process Builder                | ALL                                             | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Comply,&gt; Tools and Views,&gt; Audit Process Builder</li> <li>• Accelerators,&gt; PCI,&gt; Tools,&gt; Audit Process Builder</li> <li>• Accelerators,&gt; Data Privacy,&gt; Tools,&gt; Audit Process Builder</li> <li>• Accelerators,&gt; GDPR,&gt; Conform,&gt; Demonstrate,&gt; GDPR Data Security Compliance Review &gt; Audit Process Builder</li> </ul>                                                                                                                                                                                                                                                                                            |
| Audit Process To-Do List             | ALL                                             | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Comply,&gt; Tools and Views,&gt; Audit Process To-Do List</li> <li>• Accelerators,&gt; Data Privacy,&gt; Tools,&gt; Audit Process To-Do List</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Auditing Application                 | ALL                                             | Allows access to the following API commands: <ul style="list-style-type: none"> <li>• execute_auditProcess</li> <li>• close_default_events</li> <li>• audit_process_run_status</li> <li>• delete_audit_process_result</li> <li>• list_audit_processes</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Auto-discovery Configuration         | ALL                                             | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Discover,&gt; Database Discovery,&gt; Auto-discovery Configuration</li> <li>• Discover,&gt; Database Discovery,&gt; GIM Auto-discovery Configuration</li> <li>• Accelerators,&gt; GDPR,&gt; Assess,&gt; Discover,&gt; Data Discovery,&gt; Auto-discovery Configuration</li> </ul>                                                                                                                                                                                                                                                                                                                                                                        |
| Big Data Intelligence                | ALL                                             | Allows access to the SonarG datasource application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Catalog                              | admin                                           | Controls access to the "Catalog" domain.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| CAS Application                      | cas, admin                                      | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Harden,&gt; Configuration Change Control (CAS Application),&gt; CAS Host Configuration</li> <li>• Harden,&gt; Configuration Change Control (CAS Application),&gt; CAS Template Set Configuration</li> <li>• Harden,&gt; Reports,&gt; CAS Status</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                               |
| CAS Configuration                    | ALL                                             | Deprecated functionality.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| CAS Lost Target                      | ALL                                             | Deprecated functionality.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Central Management                   | admin, vulnerability-assess, admin-console-only | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Manage,&gt; Central Management,&gt; Central Management</li> <li>• Manage,&gt; Central Management,&gt; Portal User Sync</li> <li>• Manage,&gt; Central Management,&gt; Enterprise Load Balance,&gt; Associate S-TAPs and Managed Units</li> <li>• Manage,&gt; Central Management,&gt; Enterprise Load Balance,&gt; Enterprise Load Balance Properties</li> <li>• Manage,&gt; Central Management,&gt; Distribute Configuration Profiles</li> <li>• Manage,&gt; Central Management,&gt; Managed Unit Groups</li> <li>• Manage,&gt; Central Management,&gt; PIM Data Distribution</li> <li>• Manage,&gt; Central Management,&gt; System Resources</li> </ul> |
| Classifier                           | ALL                                             | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Discover,&gt; Classification,&gt; Discover Sensitive Data</li> <li>• Accelerators,&gt; GDPR,&gt; Assess,&gt; Discover,&gt; Data Classification,&gt; Discover Sensitive Data</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Cloud DB Service Protection          | ALL                                             | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Discover,&gt; Database Discovery,&gt; Cloud DB Service Protection</li> <li>• Accelerators,&gt; GDPR,&gt; Assess,&gt; Discover,&gt; Data Discovery,&gt; Cloud DB Service Protection</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Custom Classes                       | admin, vulnerability-assess, admin-console-only | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Setup,&gt; Custom Classes,&gt; Alerts,&gt; Delete Alerting Class</li> <li>• Setup,&gt; Custom Classes,&gt; Alerts,&gt; Update Alerting Class</li> <li>• Setup,&gt; Custom Classes,&gt; Alerts,&gt; Upload Alerting Class</li> <li>• Setup,&gt; Custom Classes,&gt; Evaluations,&gt; Delete Evaluation Class</li> <li>• Setup,&gt; Custom Classes,&gt; Evaluations,&gt; Update Evaluation Class</li> <li>• Setup,&gt; Custom Classes,&gt; Evaluations,&gt; Upload Evaluation Class</li> <li>• Setup,&gt; Custom Classes,&gt; Communication Permissions</li> </ul>                                                                                         |
| Custom Domain Builder                | ALL                                             | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Comply,&gt; Custom Reporting,&gt; Custom Domain Builder</li> <li>• Comply,&gt; Custom Reporting,&gt; Custom Query-Report Builder</li> <li>• Accelerators,&gt; Data Privacy,&gt; Tools,&gt; Custom Domain Builder</li> <li>• Accelerators,&gt; Data Privacy,&gt; Tools,&gt; Custom Query-Report Builder</li> <li>• Reports,&gt; Report Configuration Tools,&gt; Custom Domain Builder</li> <li>• Reports,&gt; Report Configuration Tools,&gt; Custom Query-Report Builder</li> </ul>                                                                                                                                                                      |

| <b>Access management application</b> | <b>Default Roles</b>                                       | <b>Access</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------|------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Custom Query Builder                 | ALL                                                        | Allows access to the following user interfaces: <ul style="list-style-type: none"><li>• Reports &gt; Report Configuration Tools &gt; Data Marts</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Custom Reporting                     | ALL                                                        | Allows access to the following API commands: <ul style="list-style-type: none"><li>• upload_custom_data</li><li>• create_custom_table_ldap_import</li><li>• update_custom_table_ldap_import</li><li>• list_custom_table_ldap_imports</li><li>• delete_custom_table_ldap_import</li><li>• run_custom_table_ldap_import</li></ul>                                                                                                                                                                                                                                                                                                                                                                    |
| Custom Table Builder                 | ALL                                                        | Allows access to the following user interfaces: <ul style="list-style-type: none"><li>• Discover &gt; Database Entitlements &gt; Entitlement Optimization</li><li>• Comply &gt; Custom Reporting &gt; Custom Table Builder</li><li>• Comply &gt; Custom Reporting &gt; Custom Table Distribution</li><li>• Accelerators &gt; Data Privacy &gt; Tools &gt; Custom Table Builder</li><li>• Reports &gt; Report Configuration Tools &gt; Custom Table Builder</li></ul>                                                                                                                                                                                                                               |
| Customer Uploads                     | admin, vulnerability-assess, admin-console-only            | Allows access to the following user interfaces: <ul style="list-style-type: none"><li>• Harden &gt; Vulnerability Assessment &gt; Customer Uploads</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Customize User/Role UI               | admin, vulnerability-assess, admin-console-only, accessmgr | Allows access to the following user interfaces: <ul style="list-style-type: none"><li>• Setup &gt; Tools and Views &gt; Customize User/Role</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Dashboard Builder                    | ALL                                                        | Allows access to the following user interfaces: <ul style="list-style-type: none"><li>• My Dashboards &gt; Create New Dashboard</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Data Access Policy Application       | ALL                                                        | Controls specialized drilldown operations for IMS Data Access, Policy Violations, Open incident, and Open incident todo list reports.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Data Management                      | admin, vulnerability-assess, admin-console-only            | Allows access to the following user interfaces: <ul style="list-style-type: none"><li>• Manage &gt; Data Management &gt; Catalog Archive</li><li>• Manage &gt; Data Management &gt; Catalog Export</li><li>• Manage &gt; Data Management &gt; Catalog Import</li><li>• Manage &gt; Data Management &gt; Data Archive</li><li>• Manage &gt; Data Management &gt; Data Export</li><li>• Manage &gt; Data Management &gt; Data Import</li><li>• Manage &gt; Data Management &gt; Data Restore</li><li>• Manage &gt; Data Management &gt; Results Archive (Audit)</li><li>• Manage &gt; Data Management &gt; Results Export (Files)</li><li>• Manage &gt; Data Management &gt; System Backup</li></ul> |
| Data Mart Builder                    | admin                                                      | Controls access to the "Datamart Extraction Log" query domain.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Data Restore                         | inv                                                        | Deprecated functionality.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Database Analyzer                    | ALL                                                        | Controls access to the Database Analyzer datasource application. Allows advanced group member import.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Database Intrusion Detection         | ALL                                                        | Deprecated functionality.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Database Security Assessment         | ALL                                                        | Allows access to the following API commands: <ul style="list-style-type: none"><li>• execute_assessment</li><li>• reset_va_summary_by_id</li><li>• reset_va_summary_by_key</li><li>• modify_va_summary_key</li><li>• get_va_summary_key</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Datasource Builder                   | ALL                                                        | Allows access to the following user interfaces: <ul style="list-style-type: none"><li>• Setup &gt; Tools and Views &gt; Datasource Definitions</li><li>• Setup &gt; Tools and Views &gt; Kerberos Configurations</li><li>• Setup &gt; Tools and Views &gt; CyberArk Configurations</li><li>• Discover &gt; Classification &gt; Datasource Definitions</li><li>• Harden &gt; Vulnerability Assessment &gt; Datasource Definitions</li></ul>                                                                                                                                                                                                                                                         |
| Datasource Group Builder             | admin, vulnerability-assess                                | Allows modification of datasource groups.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| DB2 zOS Groups                       | admin                                                      | Controls whether DB2 z/OS related groups are available for policy rule API commands.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Decision Plan Upload                 | admin, vulnerability-assess, admin-console-only            | Allows access to the following user interfaces: <ul style="list-style-type: none"><li>• Setup &gt; Tools and Views &gt; Upload Decision Plan File</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| Access management application | Default Roles                                             | Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Deployment                    | admin                                                     | <p>Allows access to the following user interfaces:</p> <ul style="list-style-type: none"> <li>• Manage &gt; System View &gt; Deployment Health Topology</li> <li>• Manage &gt; System View &gt; Deployment Health Table</li> <li>• Manage &gt; System View &gt; Deployment Health Dashboard</li> <li>• Manage &gt; System View &gt; Resource Deployment</li> <li>• Manage &gt; System View &gt; Deployment Inventory</li> <li>• Manage &gt; System View &gt; Stat Dashboard</li> </ul>                                                                                                                                                                                |
| Distributed Interface         | admin                                                     | Controls access to the "Asset event mapping" domain.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Distributed Report Builder    | admin                                                     | <p>Allows access to the following user interfaces:</p> <ul style="list-style-type: none"> <li>• Reports &gt; Report Configuration Tools &gt; Distributed Report Builder</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Express Security              | ALL                                                       | Deprecated functionality.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| externalticketing             | admin                                                     | <p>Allows access to the following user interfaces:</p> <ul style="list-style-type: none"> <li>• Setup &gt; Tools and Views &gt; External Ticketing System</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| File Activity Monitoring      | admin, fam, GDPR FAM, Internal FAM REST requests          | <p>Allows access to the following user interfaces:</p> <ul style="list-style-type: none"> <li>• Protect &gt; Security Policies &gt; Policy Builder for Files</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Global Profile                | admin, vulnerability-assess, admin-console-only           | <p>Allows access to the following user interfaces:</p> <ul style="list-style-type: none"> <li>• Setup &gt; Tools and Views &gt; Global Profile</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| GrdAPI                        | ALL                                                       | Controls whether user can execute API commands.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Group Builder                 | ALL                                                       | <p>Allows access to the following user interfaces:</p> <ul style="list-style-type: none"> <li>• Setup &gt; Tools and Views &gt; Group Builder</li> <li>• Setup &gt; Tools and Views &gt; Time Period Builder</li> <li>• Protect &gt; Security Policies &gt; Group Builder</li> <li>• Protect &gt; Security Policies &gt; Time Period Builder</li> <li>• Accelerators &gt; PCI &gt; Tools &gt; Group Builder</li> <li>• Accelerators &gt; Data Privacy &gt; Tools &gt; Group Builder</li> <li>• Accelerators &gt; Data Privacy &gt; Tools &gt; Time Period Builder</li> <li>• Accelerators &gt; GDPR &gt; Design &gt; Security by Design &gt; Group Builder</li> </ul> |
| Guardium Definitions          | admin, vulnerability-assess, admin-console-only           | <p>Allows access to the following user interfaces:</p> <ul style="list-style-type: none"> <li>• Manage &gt; Data Management &gt; Distributed Interface</li> <li>• Manage &gt; Data Management &gt; Definitions Export</li> <li>• Manage &gt; Data Management &gt; Definitions Import</li> </ul>                                                                                                                                                                                                                                                                                                                                                                       |
| Guardium Status Monitor       | admin, cli                                                | Deprecated functionality.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| IMS zOS Groups                | admin                                                     | Controls whether IMS z/OS related groups are available for policy rule API commands.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Incident Generation           | admin, vulnerability-assess, admin-console-only           | <p>Allows access to the following user interfaces:</p> <ul style="list-style-type: none"> <li>• Comply &gt; Tools and Views &gt; Incident Generation</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Inspection Engines            | vulnerability-assess, admin, admin-console-only           | <p>Allows access to the following user interfaces:</p> <ul style="list-style-type: none"> <li>• Manage &gt; Activity Monitoring &gt; Inspection Engines</li> <li>• Discover &gt; Database Discovery &gt; Database Discovered Instances Rules</li> <li>• Discover &gt; Database Discovery &gt; Database Discovered Instances Rules Scheduler</li> </ul>                                                                                                                                                                                                                                                                                                                |
| Installed Policy Viewer       | ALL                                                       | <p>Allows access to the following user interfaces:</p> <ul style="list-style-type: none"> <li>• Protect &gt; Security Policies &gt; View Installed Policy</li> <li>• Accelerators &gt; GDPR &gt; Transform &gt; Protect &gt; View Installed Policy</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                         |
| Investigation Data Restore    | inv                                                       | <p>Allows access to the following user interfaces:</p> <ul style="list-style-type: none"> <li>• Manage &gt; Data Management &gt; Audit Results Restore</li> <li>• Comply &gt; Tools and Views &gt; Audit Results Navigation</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Job Dependencies              | admin                                                     | Controls access to the "Job Dependencies" and "Job Dependencies Events" domains.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Module Installation           | admin, vulnerability-assess, admin-console-only, GDPR FAM | <p>Allows access to the following user interfaces:</p> <ul style="list-style-type: none"> <li>• Manage &gt; Module Installation &gt; GIM Processes Monitor</li> <li>• Manage &gt; Module Installation &gt; Set up by Client</li> <li>• Manage &gt; Module Installation &gt; Upload Modules</li> <li>• Manage &gt; Module Installation &gt; Upload Modules(new)</li> <li>• Manage &gt; Module Installation &gt; Centralized Module View</li> <li>• Manage &gt; Module Installation &gt; GIM Global Parameters</li> <li>• Manage &gt; Module Installation &gt; GIM Remote Activation</li> </ul>                                                                         |

| <b>Access management application</b> | <b>Default Roles</b>                              | <b>Access</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Policy Builder                       | ALL                                               | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Protect &gt; Security Policies &gt; Policy Builder for Data</li> <li>• Accelerators &gt; Data Privacy &gt; Tools &gt; Policy Builder for Data</li> </ul>                                                                                                                                                                                                                                                                                                                   |
| Policy Install                       | ALL                                               | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Setup &gt; Tools and Views &gt; Policy Installation</li> <li>• Protect &gt; Security Policies &gt; Policy Installation</li> <li>• Accelerators &gt; GDPR &gt; Transform &gt; Protect &gt; Policy Installation</li> </ul>                                                                                                                                                                                                                                                   |
| Portal Configuration                 | admin, vulnerability-assess, admin-console-only   | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Setup &gt; Tools and Views &gt; Portal</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Privacy Compliance                   | ALL                                               | Deprecated functionality.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Privacy Set Builder                  | ALL                                               | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Comply &gt; Tools and Views &gt; Privacy Set Builder</li> <li>• Accelerators &gt; Data Privacy &gt; Tools &gt; Privacy Set Builder</li> </ul>                                                                                                                                                                                                                                                                                                                              |
| Query Builder                        | ALL                                               | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Discover &gt; Database Discovery &gt; Auto-discovery Query Builder</li> <li>• Investigate &gt; Query-Report Builder</li> <li>• Accelerators &gt; Data Privacy &gt; Tools &gt; Query-Report Builder</li> <li>• Reports &gt; Report Configuration Tools &gt; Query-Report Builder</li> </ul>                                                                                                                                                                                 |
| Query Rewrite Builder                | ALL                                               | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Protect &gt; Security Policies &gt; Query Rewrite Builder</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                       |
| Quick Search                         | user, admin                                       | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Investigate &gt; Guardium Data Protection Dashboard</li> <li>• Investigate &gt; Search for Data Activity</li> <li>• Investigate &gt; Search for File Activity</li> </ul>                                                                                                                                                                                                                                                                                                   |
| Quick Start                          | admin                                             | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Setup &gt; Smart Assistant &gt; Compliance Monitoring</li> <li>• Setup &gt; Smart Assistant &gt; Compliance Health Monitor Dashboard</li> </ul>                                                                                                                                                                                                                                                                                                                            |
| Quick Start Agents                   | admin                                             | Used by Deploy Monitoring Agents feature in conjunction with Auto-discovery Configuration and Module Installation.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Remote Registration                  | user, review-only, inv, admin, admin-console-only | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Setup &gt; Central Management &gt; Registration and Load Balance</li> <li>• Setup &gt; Central Management &gt; Make Primary CM</li> </ul>                                                                                                                                                                                                                                                                                                                                  |
| Report Builder                       | ALL                                               | Controls access to the "Query Rewrite" domain. Allows REST processor access by reports.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Results Viewing                      | ALL                                               | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Comply &gt; Tools and Views &gt; Audit Results Navigation</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                       |
| Retrospective Request                | admin                                             | Controls access to the "System Audit Log" domain.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| S-Tap Management                     | admin, vulnerability-assess, admin-console-only   | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Setup &gt; Tools and Views &gt; Hadoop Monitoring</li> <li>• Setup &gt; Tools and Views &gt; IMS Definitions</li> <li>• Manage &gt; System View &gt; S-TAP Status Monitor</li> <li>• Manage &gt; Activity Monitoring &gt; S-TAP Certification</li> <li>• Manage &gt; Activity Monitoring &gt; S-TAP Control</li> <li>• Manage &gt; Activity Monitoring &gt; External S-TAP Control</li> <li>• Manage &gt; Activity Monitoring &gt; S-TAP Verification Scheduler</li> </ul> |
| Stap Reporting                       | admin                                             | Controls access to the "STAP Verification" domain.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Stap Verification                    | ALL                                               | Controls access to the "STAP Verification" datasource application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Security Assessment Builder          | ALL                                               | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>• Harden &gt; Vulnerability Assessment &gt; Assessment Builder</li> <li>• Accelerators &gt; PCI &gt; Tools &gt; Assessment Builder</li> <li>• Accelerators &gt; Data Privacy &gt; Tools &gt; Assessment Builder</li> <li>• Accelerators &gt; GDPR &gt; Assess &gt; Impact Assessment &gt; GDPR Data Security Impact Assessment &gt; Assessment Builder</li> </ul>                                                                                                            |

| Access management application | Default Roles                                   | Access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Support                       | admin, vulnerability-assess, admin-console-only | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>Manage &gt; Maintenance &gt; Support Information Gathering</li> <li>Manage &gt; Maintenance &gt; Support Information Results</li> <li>Manage &gt; Maintenance &gt; Support Maintenance</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                           |
| System Configuration          | admin, admin-console-only                       | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>Setup &gt; Tools and Views &gt; System</li> <li>Setup &gt; Tools and Views &gt; License</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| System Processes              | admin, vulnerability-assess, admin-console-only | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>Setup &gt; Tools and Views &gt; Alerter</li> <li>Setup &gt; Tools and Views &gt; Anomaly Detection</li> <li>Setup &gt; Tools and Views &gt; Session Inference</li> <li>Setup &gt; Tools and Views &gt; Data Streaming</li> <li>Manage &gt; Activity Monitoring &gt; Flat Log Process</li> <li>Manage &gt; Unit Utilization &gt; Unit Utilization Levels</li> <li>Manage &gt; Maintenance &gt; General &gt; Running Query Monitor</li> <li>Protect &gt; Database Intrusion Detection &gt; IP-to-Hostname Aliasing</li> <li>Comply &gt; Custom Reporting &gt; PIM Data Correlation</li> </ul> |
| Trigger Builder               | ALL                                             | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>Harden &gt; Configuration Change Control (CAS Application) &gt; Value Change Auditing Builder</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| UI Customization              | ALL                                             | Controls access to user-interface customization.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Workflow Builder              | ALL                                             | Allows access to the following user interfaces: <ul style="list-style-type: none"> <li>Comply &gt; Tools and Views &gt; Workflow Builder</li> <li>Accelerators &gt; Data Privacy &gt; Tools &gt; Workflow Builder</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Related concepts

- [Managing access to Guardium](#)

## Managing roles and permissions

Roles and permissions provide different levels of access to users based on their job duties.

Examples of roles include user, admin, and audit. Using roles allows you to easily define permissions for an entire group of users. Only access managers can create new roles and assign users to that role. As part of role creation, access managers can also customize the navigation menu and permissions for that role.

Creating customized roles involves several processes:

- Creating a new role
- Managing permissions for the role to limit what users can access
- Optionally customizing the navigation menu for the role to further limit what users can see
- Adding users to the role

There are two ways to limit access to specific applications:

Limit access from the application

Limit access from the application by deselecting the All Roles check box on the Role Permissions > Edit Application Role Permissions screen. Next, select the individual roles that should have access to the application.

The process is the same if you find that the All Roles check box is already deselected: simply select or deselect the individual roles to grant or revoke access to the application.

When All Roles is selected for a particular application, every currently-defined role will have access to that application.

Limit access from the role

Limit access from the role by navigating to the Role Browser > Manage Permissions screen and move individual applications from the Accessible applications list to the Inaccessible applications list.

When managing permissions or customizing the navigation menu for a new role, the defaults shown in the Accessible applications list reflects any application with the All Roles check box selected on the Role Permissions > Edit Application Role Permissions screen.

When working with roles and permissions, removing permissions for an application also changes the default permissions for new roles. That is, removing permissions for an application means that any subsequent roles you create will also lack permissions for that application. If you want a new role to have permissions for an application that no longer appears in the Accessible applications list by default, you will need to move the desired application from the Inaccessible applications list to the Accessible applications list for the new role.

It is also possible to restrict access to specific tools by hiding menu items using the Role Browser.[Customize Navigation Menu](#) tool. This approach limits access without altering the default application permissions, but it may be less secure than a permissions-based approach.

#### Best Practices:

- After editing permissions for a role, review the navigation layout for that role as shown on the Role Browser.[Customize Navigation Menu](#) screen. Add or remove items from the Navigation Menu list as needed to create a layout appropriate for the role.
- Copy and edit predefined roles to establish the desired permissions and navigation menu. This approach allows you to revert to the original role if needed.
- Be aware that when copying existing roles, whether predefined or customized, all permissions from the existing role are copied to the new role.

## Related concepts

---

- [Customizing the user interface](#)

## Related tasks

---

- [How to create a role with minimal access](#)

## How to create a role with minimal access

This topic explains how to create a new role with minimal access permissions, for example an auditor role that can only access the Audit Process To-Do List and view specific reports.

## Procedure

---

1. Create a new role.
  - a. Log in as *accessmgr*, navigate to Access.[Access Management](#), and select the Role Browser.
  - b. Click the Add Role button, give the role a name, and click the Add Role button to create the new role.
2. Manage permissions so the new role can only access the Audit Process To-Do List and the Report Builder (which is required for viewing reports).
  - a. From the Role Browser, click the Manage Permissions link for the new role.
  - b. Select the checkbox in the header of the Accessible Items list and use the arrow to move all items to the Inaccessible Items list.  
When creating a highly restricted role, it is easier to begin by removing permissions.
  - c. In the Inaccessible Items list, select the Audit Process To-Do List and the Report Builder, and use the arrow to move them back to the Accessible items list.  
The new role now has access to only these two specific applications.
  - d. Click the OK button to commit your changes.
3. Customize the menus and navigation by defining which reports and applications are available to the new role.
  - a. From the Role Browser, click the Customize Navigation Menu link for the new role.
  - b. In the Navigation Menu list, select the Reports group so it is highlighted.  
The selected group acts as the destination for menu items added in subsequent steps.
  - c. In the Available Tools and Reports list, expand the Reports section or use the Filter to identify specific reports, select the check box next to each item that should be available to the new role, and use the arrow to add the items to the Navigation Menu list.  
Items moved into the Navigation Menu list will become visible to users assigned to this role.
  - d. In the Navigation Menu list, remove access to the Report Builder by clicking the icons next to the Reports.[Report Configuration Tools](#) and Investigate groups.  
This further simplifies the menu structure for this role and removes access to the Report Builder tool without also removing application permissions that are required to access reports.
  - e. Click the OK button to commit your changes.  
You have now created a new role with very minimal privileges that can be assigned to users.
4. Optionally specify a custom home page for the new role.
  - a. From the Role Browser, click the Customize Navigation Menu link for the new role.
  - b. In the Navigation Menu list, specify a new default home page by selecting Comply.[Tools and Views](#).[Audit Process To-Do List](#) and clicking the icon in the toolbar.  
Users assigned to this role will now see the Audit Process To-Do List as the default screen after logging in.
  - c. Click the OK button to commit your changes.
5. Create a new user and add that user to the new role.
  - a. Navigate to Access.[Access Management](#) and select User Browser.
  - b. Click Add User, provide the required information, and click Add User to create the new user.  
You will now see the user you created listed in the User Browser.  
When a new user is created, the account is disabled by default. Deselect the Disabled check box if you want the user to have immediate access to their account.
  - c. From the User Browser, click the Roles link for the new user to view a list of available roles.
  - d. Select the Assign check box next to the custom role you created earlier.  
This will assign the user to the new role.
  - e. Deselect the Assign check box next to the *user* role.  
Deselecting the *user* role prevents the new user from inheriting the default *user* access and permissions.
  - f. Click Save to commit your changes.



## Related concepts

---

- [Managing roles and permissions](#)

## Managing users

Use the Access Manager, assigned the username accessmgr to add user accounts, enable or disable user accounts, import members from LDAP, or edit user permissions. Open the User Browser and browse the user accounts by clicking **Access > Access Management > User Browser**.

Defining and modifying users involves deciding both who can use the Guardium® system and in which roles. A group of users can all have the same role and the same access privileges if you so choose. For more information about roles, see [Understanding Roles](#).

You can import user definitions from an LDAP server, on demand, or on a schedule.

Regardless of how users are defined to the Guardium system, the Guardium administrator can configure the system to authenticate users by using Guardium, LDAP, or Radius.

When you get started with your Guardium system, an important early task is to identify which groups of users will use the system, along with each set of user's functions. For example, an information security group might use Guardium for alerting and troubleshooting purposes while a database administrator group might use Guardium for reporting and monitoring. As you decide who can access the Guardium system, keep in mind that sensitive company data can be picked up by the system. Therefore, you need to be aware of who can access that data.

After you decide which groups of users will use the Guardium system (and for what purpose), collect the following information for each user:

- User's first and last name
- User account name (the name they use to log in)
- User's email address
- User's country or location
- User's function or role with Guardium

## User account security

Guardium provides a number of default settings to simplify the user creation process. Several settings can be changed to provide extra security for user accounts. You can enable or disable these settings by using the show and store password CLI commands. For more information, see [User Account, Password and Authentication CLI Commands](#). Defaults are set for the following settings:

- Password validation is enabled, which means that a minimum of 8 characters is required, and the password must contain at least one character from each of the following categories:
  - Uppercase letters - A-Z
  - Lowercase letters - a-z
  - Digits - 0-9
  - Special characters, as described in [Special characters for Guardium passwords](#)
- Note: If password validation is disabled, any characters are allowed.
- Password expiration is enabled. Passwords can be configured to expire after a designated number of days.
- Account lockout that follows a specified number of failed login attempts is enabled. You can configure lockouts to occur after a fixed number of attempts in a specified time, or after a total number of attempts for the life of the account.

## Unlocking locked accounts

1. From the User Browser, click Edit for the user you want to unlock.
2. Clear the Disabled checkbox.
3. Click Update User to save changes.

If an admin or accessmgr user account is locked, an admin can unlock it with the **unlock admin** or **unlock accessmgr** CLI command. For more information, see [User account, password, and authentication CLI commands](#).

## Creating a user account

1. From the User Browser click Add User to open the User Form page.
2. Enter a unique name for User name. Do not include apostrophe characters in the name. User names are not case-sensitive.  
Note: When you add a user manually, from either the Add User page or User LDAP Import, if no first name or last name is specified, the login name is used. Non-Latin characters, such as Chinese or Japanese, are not supported in the username.
3. If smart card authentication is enabled, enter the Smart card user name.  
Tip: The smart card user name is the Common Name (CN) in the Guardium system's certificate.
4. Enter a password and confirm it again in the Password (confirm) box. The password that you assign is temporary, and the user must change it following their first login.  
Passwords are case-sensitive. When password validation is enabled (the default), the password must be 8 or more characters in length, and must include at least one character from each of the following categories:
  - Uppercase letters - A-Z
  - Lowercase letters - a-z
  - Digits - 0-9
  - Special characters, as described in [Special characters for Guardium passwords](#)
5. Enter the user's first and last name in the respective fields.  
Note: To assign a user the investigator role, the last name must be INV\_1, INV\_2, or INV\_3. While the UI does not stop you from entering a different last name, the application works properly only with these names. Furthermore, you cannot assign an investigator to any additional roles; they can be only *inv*. The *inv* role is the only case where a user or admin role is not required.
6. Optionally, enter the following information:
  - The user's email address.
  - Select the user's country or region from the menu.
  - Select Password never expires to remove password expiration. The default expiration is 90 days. Keep in mind that forcing users to change their passwords is a security feature.

7. When ready, clear the Disabled checkbox to enable access to Guardium for this user.

Note: Disabled is selected by default. Guardium suggests that you do not clear the checkbox and enable the account until after you assign the correct set of roles for the user.

8. Click Add User to save the new user account definition and close the page.

Guardium suggests that you assign all roles before you enable users so that the user has all components in their layout the first time they log in. When a user logs in for the first time, their layout is built by using all of the roles that are currently assigned. If roles are added later, the user has access to everything available to that role, but must add reports or applications particular to that role manually.

The user definition is now complete. Guardium suggests that you add the appropriate roles for the user before you inform them of their password for the initial login. For more information, see [Understanding Roles](#).

For more information on adding a user by using an API command, see [Create user](#).

## Enabling or disabling multiple users

---

Open the User Browser and click Search Users to filter users by role. When you select a user, you can enable or disable the user. Because users are disabled by default, this menu can be useful to change the status of multiple users.

Note: Guardium includes the default Guardium CLI accounts, guardcli1 through guardcli9, that are enabled by default. You can disable one or more of the default users from the User Browser or by using the `store guarduser state` CLI command.

Be sure to leave at least one guardcli account enabled to allow users to log in to the GuardAPI.

For more information about using the guardcln accounts, see [Authenticating GuardAPI commands with set guisuer](#).

## Updating a user account

---

1. From the User Browser, click Edit for the user you want to modify.

2. Replace any values in the User Form page.

3. Click Update User to save changes.

Note: If you change a user's password, the user must change it again after their next login.

## Enabling a disabled user account

---

1. From the User Browser, click Edit for the user you want to enable.

2. Clear the Disabled checkbox.

3. If the user forgets their password, enter a new password in both the Password and Password (confirm) boxes.

4. Click Update User.

## Removing a user account

---

1. From the User Browser, click Delete for the user you want to remove.

2. Click Confirm Deletion.

Note: Alerts that were sent to the deleted user are now sent to the admin; however, this change does not take effect until the access policy is reinstalled.

## Defining the data security user hierarchy

---

1. Browse to Data Security > User Hierarchy.

2. Select a user from the User menu to refresh the screen and display the selected user's current hierarchy in the user page.

3. Right-click a user node for the following options:

- Click Add User to display the Add User dialog. Search or filter by role, and add a user as a descendant of the selected user.

Defining a hierarchy can create a measure of data-level security, by allowing the parent in a hierarchy to look at specified servers and databases, but not the children in the hierarchy. Depending on the configuration, inheritance can also take place in that the parent inherits the data-level security of the child.

Note: Many-to-many relationships are allowed where a user might have more than one parent and a parent might have more than one user.

- Unlink User from parent - Sever the descendant's relationship from the parent
- Remove all descendants - Sever the relationship for all descendants from the parent

4. Click Refresh Cached Hierarchy to apply the recent changes to the user hierarchy map.

5. Click Update Active User-DB Map to apply all recent changes to the active User-DB association map.

Note: Guardium suggests that you run Update Active User-DB Map after you change the User Hierarchy.

When you change a hierarchy or to a database association, this change does not take effect automatically. The Periodic Update does not pick up the change, unless it is the first time the Periodic Update runs. For the changes to take effect, run Update Active User-DB Map.

The user hierarchy is not automatically updated. To update it, run Update Active User-DB Map. The update compares all IP addresses or Service Names to the existing hierarchy and associations to determine who has access to what.

A periodic update of the user hierarchy runs automatically every 10 minutes and cannot be run manually. The periodic update is incremental, meaning that it looks only at server IP addresses or Service Names that were added since the last time the periodic update ran. It compares the existing hierarchy and associations against the new IP addresses or Service Names and determines which users can access these IP addresses or Service Names.

## Defining the data security user-database association

---

Use the Data Security User-DB Association to find, assign, or remove users from available servers and service names (databases).

1. Open the User-DB Association window by browsing to Data Security > User-DB Association.

2. Select the checkboxes of the Server & Service Name Suggestion to find databases and service names to associate to users. Choices include:

- Observed Accesses - Observed traffic from Guardium internal database table GDM\_Access

- Datasource Definitions - Existing datasource definition information such as name, database type, authentication information, and location of datasource.
  - S-TAP Definitions - Existing S-TAP definition information such as the IP address of the database server and the IP address of the Guardium host that receives data from S-TAP.
  - Auto-Discovered Hosts - Hosts discovered by the Guardium Auto-discovery process that were not previously known. You can configure the Guardium Auto-discovery application to probe the network, searching for and reporting on all databases discovered.
  - Guardium Install Manager (GIM)-Discovered Systems - Hosts that are discovered by the GIM that are not previously known.
3. Click Go to find and display available servers, service names, and currently associated users.
- Note: When Guardium traverses the node tree, numerical indicators are displayed next to each server and service name to provide a count of direct and descendant associated users. The indicators take the format of [nn] for direct association and (mm) for descendant association (for example, when a server or service name within the current server has an associated user). Likewise, when you view users that are associated to a server or service name, if a user is associated to a larger level node in the tree, that user displays.
4. Click a server or service name node to display associated users. With any node selected, you can do one of the following tasks:
- Click Add User to add a user-DB association, click any users that you want to add, and then click Add.
  - Click Add Group to add a group-DB association. When Add Group is selected, groups that are created by using the Group Builder for group type Guardium Users display. Select the group you'd like to add and click Add.
5. Right-click any server or service name node to select one of the following tasks:
- Highlight the server.
  - Expand or collapse the server.
  - Find a server.
  - Add server, service name, or unnamed service.
  - Delete the server.
6. Add an IP address or IP/Service Name pair in the IP and Service Name fields.

Note: Use Find to search the IP/Service Name tree structure. You can enter partial IP strings or include the asterisk wildcard (\*) so that, for example, 192.168 and 192.168.\* are both valid. Numeric values cannot trail the use of any wildcard or be used with the wildcard to form an octet. Service Name names can include the wildcard % anywhere within their name.

7. Click Update Active User-DB Map to apply all recent changes to the active User-DB association map.

Note: Guardium suggests that you run Update Active User-DB Map after you change the User-DB Association.

The user hierarchy is not automatically updated. To update it, run Update Active User-DB Map. The update compares all IP addresses or Service Names to the existing hierarchy and associations to determine who has access to what.

A periodic update of the user hierarchy runs automatically every 10 minutes and cannot be run manually. The periodic update is incremental, meaning that it looks only at new server IP addresses or Service Names that were added since the last time the periodic update ran. The periodic update compares the existing hierarchy and associations against the new IP addresses or Service Names and determines which users can access these IP addresses or Service Names.

When you change a database association, this change does not take effect automatically. The periodic update does not pick up the change, unless it is the first time the periodic update runs. Otherwise, for the change to take effect, click Update Active User-DB Map.

## Managing smart card authentication

---

When smart card authentication is enabled, admin and access managers can log into the Guardium system without using a smart card. For more information, see [store system admin-only](#).

The Smart card user name is an editable field in the Guardium Portal UI that is manually populated by admins or access managers when new users are created. To authenticate a user, the Guardium system attempts to match the information on the smart card with either the User name field or the Smart card user name field.

If you upgraded your Guardium system from a previous version that did not include the Smart card user name field, the system authenticates by using the User name.

In the event that the Smart card user name is not populated but the User name is matched, the system automatically copies the value in the User name field to the Smart card user name field.

If the common name on the Guardium system's certificate is changed, the admin or access manager can manually edit the Smart card user name to match the common name. The system can then authenticate by using the Smart card user name even if the User name no longer matches.

During LDAP import, all users are imported with their existing user names. Admins or access managers can then manually add the valid common name in the certificate as the Smart card user name for authenticating by using smart cards without losing any related settings.

## Managing Guardium credentials with CyberArk

---

You can use CyberArk to manage your Guardium credentials. For more information on this application, access the CyberArk Marketplace web page and search for Guardium.

## Creating a user who can run GuardAPI commands

---

Create a user who has the proper roles and entitlements to run GuardAPI commands from the command-line interface (CLI).

### About this task

---

You can use the Guardium CLI to run both CLI commands and GuardAPI functions. This task describes how to create a user with access to the GuardAPI functions.

Note: Only the cli and guardcli1 to guardcli9 users can log in to the CLI and view or run CLI commands.

### Procedure

---

1. Log in as accessmgr to create a user who can use GuardAPI commands. Select Access > Access Management > User Browser to open the User Browser.

2. From the User Browser pane, click Add User.
3. Complete the User Form. To enable the user immediately, clear the Disabled checkbox. Click Add User to create the user. The first time the new user logs in, they must change the password.
4. From the User Browser, click Roles for the new user to display the User Role Form pane.
5. Select CLI, along with any additional roles that the user requires.  
Note: Many GuardAPI commands are associated with specific applications and their roles. That is, only a user with the accessmgr role can view and run access management commands (such as `create_user`).
6. Click Save to grant the specified roles to this user.

## What to do next

---

After you create a user with the CLI role (along with any other roles they need), that user can log in and use the CLI as follows:

1. From the CLI, log in as one of the `guardcli` users (that is, `guardcli1` to `guardcli9`). For example:

```
ssh guardcli2@company.com
```

2. Run the `set guouser` CLI command to associate the new user with the `guardcli` user. The first time the user logs in, they are prompted to change their password. For example, if you created a user with CLI privileges for Hadrian Swall:

```
company.com> set guouser Hadrian.Swall
Enter current password:
First login as Hadrian.Swall. Please change the default password.
Enter new password:
Re-enter new password:
ok
```

For more information about `set guouser`, see [User Account, Password, and Authentication CLI Commands](#).

3. The user, Hadrian Swall, can now access to any GuardAPI commands that are available for the associated roles.

## Related concepts

---

- [Using GuardAPI commands](#)
- [User Account, Password, and Authentication CLI Commands](#)

## Related reference

---

- [Guardium API A-Z Reference](#)

## Importing users from LDAP

---

You can import Guardium® user definitions from one or more LDAP servers by configuring an operation that imports the set of users who need Guardium access.

You can run the import operation on demand, or schedule it to run on a periodic basis. You can elect to import only new users, or replace existing user definitions. In either case, LDAP groups can be imported as Guardium roles.

When you import LDAP users,

- The Guardium admin user definition is not changed in any way.
- Existing users are not deleted unless you select the Delete user if not on the import list option.
- Guardium passwords are not changed.
- New users who are added to Guardium:
  - Are marked inactive by default.
  - Have blank passwords.
  - Are assigned the user role.

Notes:

- You cannot use special characters in usernames.
- When you add a user manually via access management (either from Add User or LDAP user import), if no given name or surname is provided, the login name is used.

## Configuring the LDAP server connection

---

To open the LDAP User Import page, browse to Access > LDAP User Import from the Guardium access manager.

Note: To configure LDAP user import, the accessmgr user must have privileges to run the group builder. In certain situations, when changes are made to the role privileges, accessmgr's privilege to group builder can be removed. In this case, you cannot save or run LDAP user import. From the access management portal, select Role Permissions. From Group Builder, select Roles. Make sure that either All Roles or accessmgr is selected.

1. To configure an LDAP server for user import, click  to open the Create LDAP Configuration window. In the LDAP Config tab, enter the following information:

- LDAP host name - The IP address or host name for the LDAP server to access.
- Port - The port number for connecting to the LDAP server.
- Server type - The LDAP server type.
- Use SSL connection - Select if Guardium connects to your LDAP server using an SSL (secure socket layer) connection.
- Base DN - The node in the tree at which to begin searching for the LDAP server. The following example shows a Base DN entry for a company tree,

```
DC=encore,DC=corp,DC=root
```

- Log in as and Password The user account information that is needed to connect to the LDAP server.
- Search Filter Scope - Defines the search level. Select One-Level to apply the search to the base level only, or select Sub-Tree to include levels underneath the base level.
- Import Limit - The maximum number of items to return. Guardium recommends that you use this field only to test new queries or modifications to existing queries so that you do not inadvertently load an excessive number of members.
- Search Filter - Defines a base DN, scope, and search filter. Typically, imports are based on membership in an LDAP group, so you want to use the memberOf keyword. For example,

```
memberOf=CN=syyTestGroup,DC=encore,DC=corp,DC=root
```

- Disable user if not on the import list - Allows you to automatically disable users who are not explicitly added to Guardium.

2. Click Test Connection to test the connection to the LDAP server, and then Save to save your changes.

## Configuring the import process

---

After you configure the connection to the LDAP server, select the Import Config tab to configure the process of importing users and roles from LDAP.

In the Import Config tab, enter the following information to import users:

- LDAP host name - The IP address or host name of the LDAP server (from the LDAP Config tab).
- Domain - A unique identifier for this LDAP server. The same user ID (sAMAccountName) might exist in more than one domain, so Guardium needs a way to distinguish between the users in separate domains. If an existing user is already loaded from another domain, the current LDAP domain is appended to the username from LDAP to create the Guardium user: <user>@<domain>. In general, do not update the LDAP server domain after you import users because the domain might be part of the username. If you do update the LDAP server domain, Guardium updates any usernames from the old domain to the new domain (that is, from user@old\_domain to <user@new\_domain>).

Note: If your site is upgrading to Guardium 11.4 or later, you must populate the domain field after the upgrade.

- Import mode - If you choose to import existing users, then select whether to keep or override the existing attributes for those users.
- Delete user if not on the import list - Delete existing Guardium users who were previously imported from the same LDAP server, but are no longer in LDAP. Use this option to help keep Guardium users in sync with the LDAP server.
- Enable new imported users - Enable users as soon as they are imported. If you do not select this option, then enable new users from the access manager User Browser.
- User RDN Type - LDAP users are identified by the User RDN Type. The default User RDN type is *uid*. However, work with your Guardium administrator to determine what value to use.

Note: The following RDN values require special processing:

- For *uid* - Always specify the RDN type as *uid=search*. For example,

```
uid=search
```

- For *sAMAccountName* - Specify the RDN type as either *=search* or *=[domain name]* in the users' full names. For example,

```
sAMAccountName=search, sAMAccountName=dom
```

- Object class for user - Search filter for object class of user DN in LDAP. For example,

```
(objectClass=organizationalPerson) (objectClass=inetOrgPerson) (objectClass=person)
```

For more information, see [Configuring authentication](#).

Note: For any option that includes the  icon, click  to enter the default values.

To also import LDAP roles, select Import roles and then enter the information that you need:

- Overwrite existing user roles - Synchronize user roles in Guardium with the role assignments in LDAP. Guardium internal roles are not updated or changed.
- Attribute to import as role - The attribute to use for importing roles, such as CN. Each attribute has a name and belongs to an objectClass.
- Role Search Base DN - The node in the tree at which to begin searching for roles. For example,

```
OU=groups,DC=encore,DC=corp,DC=root
```

- Role Search filter - The search filter for roles.
- Object class for role - The search filter for the object class of role DN in LDAP. For example,

```
(objectClass=groupOfNames) (objectClass=group) (objectClass=groupOfUniqueNames)
```

- Attribute in user to associate role - The attribute of user DN in LDAP that contains the user's role entries. For example, `memberOf`.
- Attribute in role to associate user - The attribute of role DN in LDAP that contains the member entries. For example, `member`.

When you are done, click Test Connection and then click Save.

## Running an LDAP Query

---

After you configure LDAP or the import process, click Query LDAP to run a query against the selected LDAP server with any selected filters. The results display in the LDAP Query Result tab.

From LDAP Query Result, you can select one or more users to import into Guardium.

To import users from LDAP Query Result:

1. Run an LDAP query from either the LDAP Config or Import Config tabs.
2. From LDAP Query Result, select one or more users (or all users), and click  to import the selected users.

## Scheduling LDAP user import

---

After you configure the LDAP user import, you can create an import schedule.

1. From LDAP User Import, click Schedule to open the LDAP user import schedule window.
2. Create a schedule for importing LDAP users and roles. For more information about creating a schedule, see [Scheduling](#). Select Run Once Now to import LDAP users immediately.

## Deleting an LDAP connection

To delete an LDAP server connection, select the connection that you want to delete, and click .

**CAUTION:**

If you delete an LDAP server connection, you also delete all of the users who are imported from that server.

Guardium suggests that instead of deleting a server, you update the configuration. Select the server that you want to update and click .

## Data Security - User Hierarchy and Database Associations

You can use data security features to create a hierarchy of users and associate users to specific databases and servers. Guardium® data security features report on which users accessed what information, and ensure that only specific users see information that they are responsible for.

Follow these steps to enable and use Guardium data security features:

1. Enable Data Security
2. Create a User Hierarchy
3. Create a User to Database Association
4. Filter Results

When data security features are used with the Classification feature (which discovers and classifies sensitive data found in multiple places of the database), the Data Level Security prevents a specified user from seeing classifier results from a specified datasource (datasource definition). Using Data Level Security can also prevent a specified user from seeing Audit Task results when the task type is Classifier.

## Enable Data Security

Restriction: Data Level Security and the Investigation Dashboard cannot be enabled concurrently.

1. Log in as the admin user and open the Global Profile by clicking [Setup > Global Profile](#).
2. Click Enable for Data level security filtering.

Note: The status indicator icon for Data level security filtering will now appear as .

You can verify that Data level security filtering is enabled by referencing the Services Status panel ([Setup > Services Status](#)).

- With data level security filtering enabled, log in as the accessmgr to use the User Hierarchy and User-DB Association features.

## Create a User Hierarchy

The User Hierarchy shows you the parent-child relationships between all users. User hierarchies permit the parent of the relationship to look at specified servers and databases, but not the children.

Log in as accessmgr and open the User Hierarchy by clicking [Data Security > User Hierarchy](#).

Do one of the following:

- Click Update Active User-DB Map to view the full hierarchy of users.
- Use the Roles and Users filters to view the hierarchy for a specific user or role. Right-click a node in the hierarchy to expand or collapse the tree, or add a user to a specific hierarchy.
- Click Refresh Cached Hierarchy to update the hierarchy.

Note: Depending on the configuration, inheritance can also take place where the parent inherits the data-level security of the child.

## Create a User to Database Association

The User-DB Association feature maps users to specific databases to ensure that users see only data that they are permitted to view.

Log in as accessmgr and open the User-DB Association by clicking [Data Security > User-DB Association](#).

Do one of the following:

1. View the current mapping of users to databases by clicking Update Active User-DB Map.
2. Create a new User-DB association map by selecting options from the Server & Service Name Suggestion list and clicking Go.

Note: Once the map is updated, you will see a tree listing all your servers. Click any node in the tree to view which users are currently associated with that node. If you are using dual-stack configuration, there is a root node, and two trees of addresses to choose from. One tree is for the IPV4 address, and the longer tree is for the IPV6 address.

Add a user or group to a node by selecting the node and clicking Add user or Add group.

## Central Management

On a Central Management appliance, there is also a box on the User-Database Associations screen that allows a user to create database associations based on data from a managed node. Select a remote source from only a box that appears for Central Management appliances. Also, there is a check box to get data from ALL managed nodes.

## Filter Results

Data level security at the observed data level requires the filtering of data for specific users and the specific databases they are responsible for.

Filtering at the system level is based on the User Hierarchy and User-DB Association so that users will see only information from their assigned databases for the various reports, audit processes, security assessments, and so on, within the Guardium system.

Log in as the admin user and use the Global Profile to filter results. Open the Global Profile by clicking [Setup > Global Profile](#).

- Default filtering:
  - Show all - This option is available only if the user logged in has the special role *datasec-exempt* defined, which allows the user to see all data as if there was no data level security.
  - Include indirect records - This check box shows the viewer not only the rows that belong to the user logged in, but also all the rows that belong to other users within that hierarchy.
- Audit Process Escalation: Escalation is allowed for tasks on this type only to users who have the *datasec-exempt* role. Users without the *datasec-exempt* role are not shown in the escalation list.  
Escalate results to all users - A check mark in this check box escalates audit process results (and PDF versions) to all users, even if data level security at the observed data level is enabled. The default setting is enabled. If the check box is disabled (no check mark in the check box), then audit process escalation only will be allowed to users at a higher level in the user hierarchy and to users with the *datasec-exempt* role. If the check box is disabled, and there is no user hierarchy, then no escalation is permitted.
- PDF and CSV generation for results (attached to email) distribution will use the default global profile values set in Administration Console parameters.
- PDF and CSV generated from the viewer will use the same filtering as in the screen.

Note:

The Data Security User to Database Association filters reports only from the following domains: Access; Exception; and, Policy Violations (as well as custom domains using these domains or tables from these domains). All other domains (reports) are not filtered by the Data Security User to Database Association.

Users with admin role will be able to see event types on all roles (the information will still be filtered based on observed data level security parameters).

If Data Level Security is turned on, predefined entities added to a custom domain need to be in the same domain(s) for the data level security filtering to work properly.

If Data Level Security is on, and two predefined entity subjects are trying to send data from two domains (not Custom Domains) that are using a filtering policy, then the sending of the two predefined entity subjects will not be permitted. Data Level Security can only enforce one kind of filtering policy (for example, there can be only one policy depending on server\_ip/service\_name and one policy depending on datasource).

## How to define User Hierarchies

Use the UI from an access manager account to easily define user hierarchies.

### About this task

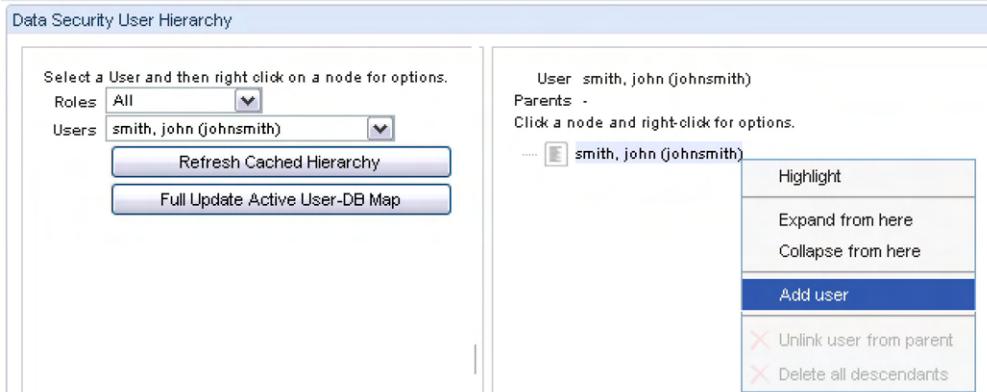
The Data Security User Hierarchy represents the parent-child relationships between users; allowing for the creation and enforcement of a data-level security by permitting the parent of a hierarchy to look at specified servers and databases, but not the children. Depending on the configuration, inheritance can also take place in that the parent inherits the data-level security of the child.

### Procedure

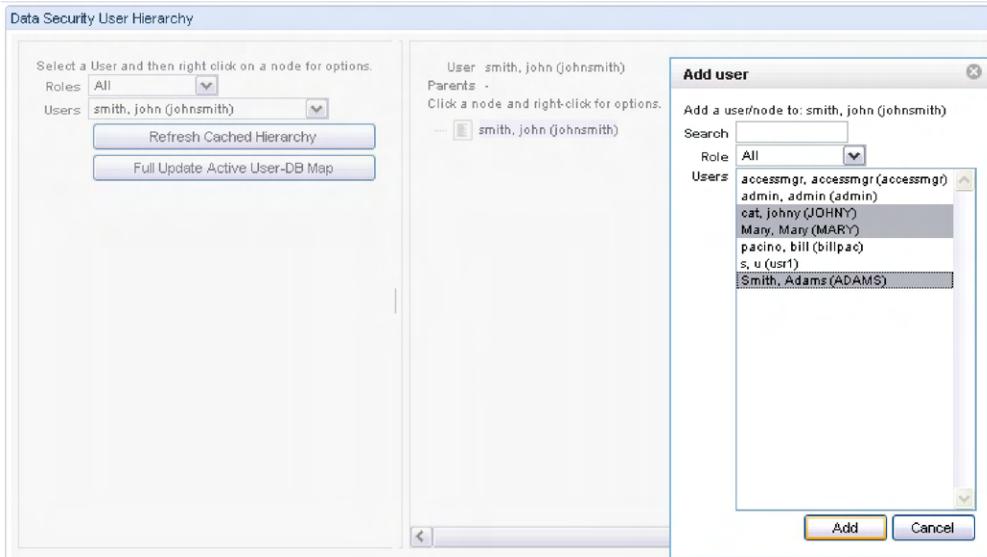
1. Login as accessmgr and click [Data Security > User Hierarchy](#).
2. Select a user from the Users drop-down menu to display it in the Data Security User Hierarchy pane. This example uses john smith as a user.

The screenshot shows the 'Data Security User Hierarchy' interface. On the left, there's a search bar with the placeholder 'Select a User and then right click on a node for options.' Below it are dropdown menus for 'Roles' (set to 'All') and 'Users' (set to 'smith, john (johnsmith)'). There are two buttons at the bottom of this panel: 'Refresh Cached Hierarchy' and 'Full Update Active User-DB Map'. On the right, the user 'smith, john (johnsmith)' is listed under 'User'. Below it, it says 'Parents - Click a node and right-click for options.' followed by a tree structure starting with '... smith, john (johnsmith)'.

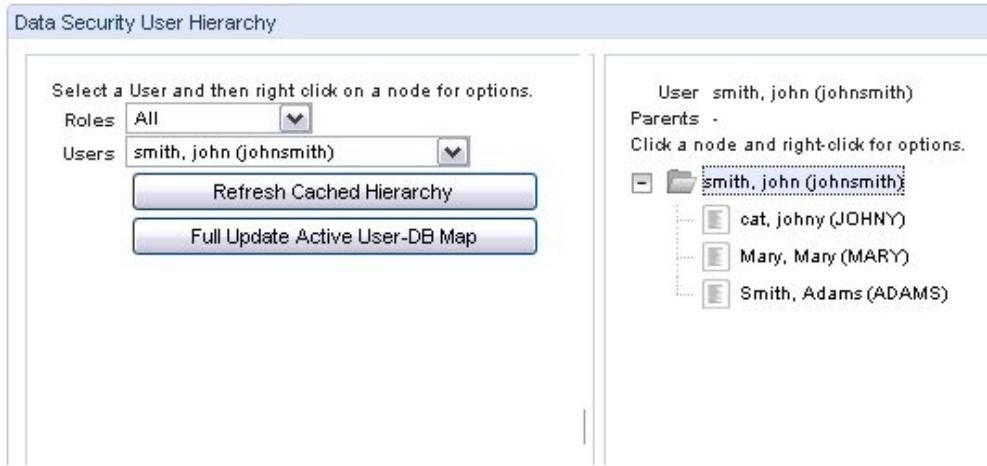
3. To add a user to john smith's hierarchy, right-click on the user in the Data Security User Hierarchy pane, and select Add user from the drop-down menu.



4. After clicking Add user from the drop down list, the Add user dialog appears. Select one or more users that you would like to add to the user's hierarchy, and then click Add.



5. After adding the users to a hierarchy, the Data Security User Hierarchy panel will be refreshed; allowing the user to drill down and see the new hierarchy.



6. Repeat the steps until all required users are defined to the data security user hierarchy.

## Central Management

In a central management configuration, one Guardium® unit is designated as the Central Manager. That unit can be used to monitor and control other Guardium units, which are referred to as managed units. Unmanaged units are referred to as stand-alone units.

The concept of a local Guardium system can refer to any Guardium system in the Central Management paradigm. Some applications (Audit Processes, Queries, Portlets, etc.) can be run on both the managed units and the central manager. In both cases, the definitions come from the Central Manager, and the data comes from the local Guardium system (which might also be the central manager).

After a Central Management system is set up, you can use either the central manager or a managed unit to create or modify most definitions. Keep in mind that most of the definitions are stored on the central manager, regardless of the system that does the actual editing.

Note:

- With the Remote Source function, a user on the manager can: run any report on the managed unit (the user must have the correct role privileges); and view data and information of that managed unit.
  - CAS template definitions are shared between all units of a federated environment just like all other definitions (reports, policies, alerts, and so on).
  - It is recommended that a user run CAS Reports on a manager, especially CAS Reports relating to CAS configurations, hosts, and templates.
  - If you create a report with the Custom Domain Builder, and some or all of the tables are remote (they are stored on the manager, such as Datasource or Comments), this report does not work on a managed node. No data is returned.
  - The Central Management page of a manager does not automatically refresh itself based on a specific interval. It times out based on the GUI timeout of the system.
  - After some time of inactivity, the system logs you out automatically and displays a sign-in dialog. The length of the GUI timeout can be set with the CLI command **store session timeout** (default is 900 seconds). View the timeout with the CLI command **show session timeout**. Status lights refresh every 5 minutes when the session is active.
  - To synchronize or upload any data from the Central Manager to managed nodes, all nodes that are involved in this type of activity MUST be on the SAME version of Guardium.
  - During the Central Management Redundancy Transition, it can take up to 5 minutes for the Unit type sync to occur depending on how many units are defined in the central management environment.
  - IPMODE information is shared with the central manager at registration. A managed unit that registered with the central manager in a pre-V11.2 release is not aware of its IP mode and cannot share that information with the central manager. Even if a managed unit was upgraded to V11.2 and later, it does not share its IP mode with the central manager, unless you unregister and reregister it. To rectify: In the Central Manager page, select individual managed units, or all managed units, and click Refresh Unit info.
- Guardium Component Services**
- Identify Guardium components and the locations from which they are taken in a central management environment.
- That unit can be used to monitor and control other Guardium units, which are referred to as managed units. Unmanaged units are referred to as stand-alone units.

Table 1. Guardium Component Services

| Component                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Users, Roles and Permissions | <p>Central Manager controls the definition of users, roles, groups and datamart tables for all managed systems. The Central Manager exports the complete set of user, security role, group, and datamart tables definitions on a scheduled basis or on demand. The managed units update their internal databases on an hourly basis. As a result, there might be a delay of up to an hour between the time users, roles, permissions or datamart tables are added or modified on the Central manager and the time that the managed unit applies those updates.</p> <p>Note: If you have Guardium® users or security roles that are defined on an existing stand-alone unit that is about to be registered for central management, those definitions will not be available after the system is registered, unless those users and security roles have also been defined on the Central Manager. You cannot administer users or security roles on a managed unit. Those definitions can be administered only when logged on to the Central Manager. When a unit is unregistered for central management, all added users and security roles are removed leaving only the default users (admin, accessmgr). When installing an Accelerator add-in product (PCI, SOX, etc.), in a Central Manager environment, install it first on the Central Manager and then on the managed unit. Add any roles and users as required for the Accelerator on the Central Manager (and those will be synchronized with the managed unit from there). Accelerator documentation is contained within the Accelerator module. See an overview of PCI Accelerator at the end of this Component Services table.</p> |
| Aliases and Groups           | On all processes that automatically generate aliases or groups, for example: import user groups from LDAP, group generation from queries, alias generation from queries, classifier, etc. if the same group or alias is automatically generated on more than one managed machine (managed by the same manager), then it might conflict with an existing group or alias, which will not be replaced.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Audit Processes              | The definitions of the Audit Process itself and all of its corresponding tasks are saved to the Central Manager and available to all managed units. However, Schedules, Results, and To-Do lists are saved on the local machine. This means that the same Audit Process tasks can be run on all Managed Units, plus the Central Manager. But it can be run at different times on different machines, which can be useful if the Managed Units have different peak load periods. Each machine has its own set of results, which are based on the data that the machine has collected; and each machine has its own set of To-Do lists for all users. Audit Process definitions are exported from the Central Manager to the managed units as part of the user synchronization process (see Synchronizing Portal User Accounts). When audit process results have been produced, the results are available to users, but on managed units, there might be a delay of up to an hour before reports or monitors such as Outstanding Audit Process Reviews are updated.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Queries                      | Each query can get only database information from a single machine. Queries that require access information including both Central Manager definitions and Managed Unit data show no data, or missing data.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Policies                     | Policy definitions are saved on the Central Manager. However, when you install a policy on a Managed Unit, a local copy is made and saved on the Managed Unit. The reason for that is that the Managed Unit is needed to keep on monitoring the database activity and using the policy even when the Central Manager is not available for any reason.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                              | <p>Note: Installing a policy on a managed node will not upload this policy to the Central Manager until the Refresh on the Central Manager is clicked. Versions must be the same between Central Manager and Managed Unit when installing policies else policies will not install and errors are generated.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

| Component                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reports                        | <p>Report definitions are saved on the Central Manager.</p> <p>When regenerate portlet is called on a Central Manager, it also sends a management (https) request to all managed units to regenerate the portlet (with the report ID). When regenerate is called on a managed unit - if it is called from the screen (not the management request), then it should send a management request to the manager to refresh the portlet (this would also send it to all units). There is a persistence mechanism for management requests for the case a unit is down - see sections within this topic on registration and policy installation.</p> <p>From the Central Manager, reports and audit processes can use data from a managed unit but not managed aggregators. The managed unit is selected as a run-time parameter, is referred to as a remote datasource, and presented as a filtered drop-down selection list containing only managed units. When an audit process references a remote datasource, that audit process can be run from the Central Manager only, so it will not appear in a list of audit processes that are displayed on a managed unit.</p> <p>Note: Certain reports, on a Central Manager, of domain Sniffer Buffer Usage (for example, Request Rate, CPU Usage, Buffer Usage Monitor) will NOT display any data. The reports will be empty.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Security Assessment            | Like the Audit Process, the definition of the Security Assessment itself is saved to the Central Manager. But the results are saved on the local machine. This means that the same Security Assessment can be run on all Managed Units, plus the Central Manager.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Comments                       | Comments can be saved on either the local machine or the Central Manager, depending on what the comment is associated with. If the Comment is associated with a definition that resides on the Central Manager, then it is also saved on the Central Manager. If the Comment is associated with a Result on the local machine, OR something specific to a Managed Unit (like an Inspection Engine), the Comment is also saved on the local machine.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Schedules                      | Schedules are always saved on the local machine, even when the definition is saved on the Central Manager.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Non-Central Manager Tasks      | When a server is configured as a Central Manager, you must be aware of the tasks that cannot be performed on that unit, but rather must be performed on other (non-Central Manager) units. Inspection engines cannot be defined on the Central Manager and can be created only on the Managed Units. But Inspection engines can be viewed from the Central Manager.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Upgrade Considerations         | It is recommended to have your Central Manager and managed units on the same version. The Central Manager should be upgraded first and then the managed units should follow. Having a manager in a different version than its managed units should be a temporary thing and it is highly recommended to upgrade all managed units to the same version as the manager. Run Sync (Refresh) on all managed nodes after upgrading, in order for these managed nodes to recognize the proper software version that they are.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| PCI Accelerator for Compliance | <p>The PCI Data Security Standard consists of twelve basic requirements. Much of the requirements are focused on protecting physical infrastructure (for instance, Requirement 1: Install and maintain a firewall configuration to protect data) or implementing procedural best practices (for instance, Requirement 5: Use and regularly update anti-virus software). However, an extra emphasis is placed on real-time monitoring and tracking of access to cardholder data and continuous assessment of database security health status (for instance, Requirement 10: Track and monitor all access to network resources and cardholder data).</p> <p>Guardium's PCI Accelerator for Database Compliance is tailored to simplify organizational processes that are needed to support these monitoring and tracking mandates and to allow for cardholder data security. The Accelerator report templates can be customized to directly reflect specific organizational and regulatory requirements. You can access these templates using the tabs that are provided:</p> <ul style="list-style-type: none"> <li>• PCI Data Security Standard overview</li> <li>• Plan and Organize</li> <li>• PCI Req. 10: Track and Monitor Access</li> <li>• PCI Req. 11: Regularly Test and Validate</li> <li>• PCI Policy Violations Monitoring</li> </ul> <p>Other tools in the Guardium family of solutions are available to help meeting regulations include the following:</p> <ul style="list-style-type: none"> <li>• PCI Compliance Report Card - A detailed view of cardholder databases access security health that is used to automate the compliance processes with continuous real-time snapshots customized for user-defined tests, weights, and assessments. The Report Card can be generated using security assessment.</li> <li>• Full Audit Trail - The non-intrusive generation of a full audit trail for data usage and modifications that are required by regulatory compliance.</li> <li>• Automated Scheduling - Automated scheduling of PCI work flows, audit tasks, and dissemination of information to responsible parties across the organization.</li> </ul> |

The following table can help identify which components are taken from which location in a central management environment.

Table 2. Components and Location in Central Manager Environment

| Central Manager              | Managed Unit                     |
|------------------------------|----------------------------------|
| Users                        | System Configuration             |
| Security Roles               | Inspection Engines               |
| Application Role Permissions | Alerter (configuration)          |
| Queries                      | Anomaly Detection                |
| Reports                      | Session Inference                |
| Time Periods                 | IP-to-Hostname Aliasing          |
| Alerts                       | System Backup                    |
| Security Assessments         | Aggregation / Archiving          |
| Audit Process Definitions    | Custom Alerting                  |
| Privacy Sets                 | Custom Identification Procedures |
|                              | Exported csv Output              |
| Policies                     | Schedules                        |
| Groups                       | DB Auto-discovery Configurations |
| Aliases                      | Audit Process Results            |

Users, Security Roles, Audit Process Definitions, and Groups are exported from the Central Manager to all managed units on a scheduled basis, as described later.

From the Central Manager, the administrator can:

- Register Guardium units for management
- Monitor managed units (unit availability, inspection engine status, etc.)

- View system log files (syslogs) of managed units
- View reports using data on managed units
- View main statistics for managed units
- Install Guardium security policies on managed units
- Restart managed units
- Manage Guardium inspection engines on managed units
- Maintain the complete set of Users, Security Roles, Groups, and Application Role Permissions that are used on all managed systems
- Patch distribution
- Distribute Uploaded JAR files
- Distribute Patch Backup Settings
- Distribute Authentication Config
- Distribute Configurations

Note: Application Role Permissions can also be changed by the administrator from any managed unit. When this happens, the permissions are changed for all managed units.

---

## Implementing Central Management

Make one machine into a Central Manager, connect the other machines into a Central Management system, and register the Managed Units to communicate with the Central Manager.

- Implementing Central Management in a New Installation
- Implementing Central Management in an Existing Installation
- If the Central Management Unit is unavailable
- **Implementing Central Management in a New Installation**  
Make one Machine the Central Manager, use the same shared secret, register units, and group managed units.
- **Implementing Central Management in an Existing Installation**  
Implement Central Management in an existing Guardium environment and migrate a CAS collector with active instances to be managed.

---

## Implementing Central Management in a New Installation

Make one Machine the Central Manager, use the same shared secret, register units, and group managed units.

### Make one machine the Central Manager

The first thing is to make one machine into a Central Manager. Select a machine. Then, complete the following steps.

1. Log in to the CLI of the Machine that you want to make the Central Manager.
2. Enter store unit type manager. This step makes the machine a Central Manager; however, it is not yet managing anything.

### Use the Same Shared Secret

After you have a Central Manager, you must connect the other machines into a Central Management system. For security reasons, it is a requirement that the communications between the machines be encrypted by using the same shared secret. To do this step, do the following action items.

1. Click Setup> Tools and Views> System to open System.
  2. Set the shared secret to the same string on all systems.
- **Registering Units**  
Register managed units to communicate with the Central Manager.
  - **Unregistering a Managed Unit**  
When a unit is unregistered, always unregister from the Central Manager. This method is the only way that the Central Manager decrements its count of managed units.
  - **Synchronizing Portal User Accounts**  
Manage portal user synchronization by using the Central Manager.

---

## Registering Units

Register managed units to communicate with the Central Manager.

You can register Guardium units for central management either from the Central Manager or from the unit itself. Regardless of how the registration is done, the Central Manager and all managed units must have the same system shared secret. If the unit to be managed is already registered for central management with another manager, unregister the unit from that central manager before you register it with the new manager. Be sure to understand exactly what happens to that unit when it is registered and unregistered for central management.

Note: If the user that is logged in to a managed unit does not exist on the Central Manager, the session is invalidated. It remains invalidated until the unit is registered with a Central Manager.

### What Happens during Registration

The following actions happen on registration.

- The unit type is set to managed and manager IP is stored.
- Product key of manager is applied. (License key is not propagated with Ping or User sync. It is sent on registration or when the system refreshes.)
- All job scheduling is reset to default.
- All psml files (portal GUI customizations) are removed.
- All local users and roles are removed.
- List of threshold alerts that is not be evaluated is reset.
- Users roles, permissions from manager are loaded.
- Custom classes, user uploaded JARs, LDAP truststore from manager are uploaded.
- Database connection from managed to manager is enabled.
- Database connection from manager to managed is enabled.
- CAS listener is started if needed.

After registration all definitions of reports, queries, groups, policies, audits, and more are retrieved from the Central manager.

Attention: When registering a standalone system that was previously used for data-access monitoring or vulnerability assessment, export any content from that system that you want to preserve and then import that content after completing registration with the central manager. This may include any of the following definitions:

- Policies and groups
- Queries and reports
- Security assessments
- Datasources
- Data marts
- Dashboards

For more information, see [Exporting and importing definitions](#).

## If the Registered Unit Status Remains Offline

---

If you know the unit that is registered is online and accessible from the Central Manager, but its status remains offline, then complete the following steps.

- Verify that the unit to be managed is online, accessible, and operational by using a browser window to log in to the Guardium system on that unit.
- Click Refresh for the unit.
- Check that you entered the correct IP address for the unit.
- Check that the unit has the same shared secret as the Central Manager.

Note: If the registration of a unit is offline, the registration request persists. It is resent to the IP/port specified on a set interval until the unit registers. A registration request that does not succeed expires after seven days.

## Registering from a Managed Unit

---

On a managed unit, you can use the GUI to register the unit with the Central Manager. Otherwise, you can use the CLI register command as described in Registering a Managed Unit with the CLI.

1. Click Setup > Central Management > Registration and Load Balance to open Central Management Registration.
2. For Host IP, enter the IP address of the Central Manager.
3. For Port, enter the https port for the Central Manager (usually 8443).
4. Click Register.

After you register on the managed unit, it initiates communication with the Central Manager, and nothing more needs to be done.

Note: The central management unit must be online and accessible by this unit when you register for central management. In contrast, when you register units for management from the central management unit, you can register units that are not currently accessible.

## Registering a Managed Unit with the CLI

---

1. On the managed unit, log in to the CLI.
2. Type register management <Manager IP> <Manager Port>

After you register on the managed unit, it initiates communication with the Central Manager, and nothing more needs to be done.

## Registering units from the Central Manager

---

You can register units that are not currently accessible.

1. Navigate to Manage > Central Management > Central Management to open Central Management.
2. Click Register New. The unit Registration page opens.
3. Enter the Unit IP and port, and click Save. The Central Management page refreshes with the new unit.

## Unregistering a Managed Unit

---

When a unit is unregistered, always unregister from the Central Manager. This method is the only way that the Central Manager decrements its count of managed units.

Unregistering from the managed unit does NOT unregister the unit on the Central Manager. The Central Manager still counts that unit as a managed unit for licensing purposes and treats the unit as managed. It might not allow another unit to be registered with the Central Manager. The unregister function on the managed unit is included for emergency use ONLY. If a manager is no longer in service, then you must unregister the unit before you can register it to another manager.

If you unregister a unit from the managed unit, it still shows on the Central Manager screen. Pressing refresh for that unit reregisters it. Pressing any other operation for that unit gives out a message that the unit is no longer managed and removes it from the manager.

On a managed unit, you can use the GUI to unregister the unit with the Central Manager. Also, you can use the CLI unregister command as described in Unregistering a Managed Unit with the CLI.

1. Log in as admin to the Guardium UI of the unit to be managed.
2. Click Set > Central Management > Registration and Load Balance to open Central Management Registration.
3. Click Unregister.

## What Happens during Unregistration

---

The following actions take place upon unregistration.

- The unit type is set to standalone.
- The manager IP is cleared.
- The product key is cleared (license is null until registration to new manager or a license is loaded manually).
- The list of threshold alerts that is not evaluated is reset.
- All job scheduling is reset to default.
- Psml files are removed.
- All users but the default users (admin, accessmgr) are removed.
- The database connection from managed to manager is disabled.
- The GUI is restarted.

After unregistration all definitions of reports, queries, groups, policies, audits, and more are retrieved from the local database, the definitions that are stored on Central Manager are no longer accessible.

If you are unsure about how to verify, contact Guardium Support before you unregister the unit.

## Unregistering a Unit from the Central Manager

---

1. Log in, as admin, to the Central Manager.
2. Click Manage > Central Management > Central Management to open Registration.
3. Mark the check box for the managed unit you want to unregister.
4. Click Unregister.

Unregistering a managed unit from the Central Manager screen removes it from the managed unit list and sets the unit to be a stand-alone unit.

Note: The product key of the unit is removed and unless the unit is registered to another manager the product key is placed in manually.

## Unregistering from a Managed Unit

---

On a managed unit, you can use the UI to unregister the unit with the Central Manager. Also, you can use the CLI unregister command as described in Unregistering a Managed Unit with the CLI.

1. Log in, as admin, to the managed unit.
2. Click Setup > Central Management > Registration and Load Balance to open Registration.
3. Click Unregister.

To unregister a Managed Unit by using the CLI, complete the following steps.

1. On the Managed Unit, log in to the CLI.
2. Enter `unregister management`.

After you have unregistered from the Managed Unit, it severs communication with the Central Manager, and nothing more needs to be done.

## Synchronizing Portal User Accounts

---

Manage portal user synchronization by using the Central Manager.

### About this task

---

As mentioned earlier, the Central Manager controls the definition of Users, Security Roles, Groups, and datamart tables for all managed units. The Central Manager makes an encrypted and signed copy of its complete set of User and Security Roles. In addition, the Central Manager transmits that information to all managed units. Furthermore, some other definitions that are required for local processing (Groups and Group members, Audit processes, Aliases, and more) are also copied. The managed units then update their internal databases on an hourly basis. This process means that there might be a delay of up to an hour before using these roles or datamart tables.

A full user synchronization cycle occurs on registration or by pressing Refresh from the Central management screen. In both cases, the synchronized information is sent from the manager and loaded on the managed units immediately.

Note: Use caution when setting the schedule so that it does not interfere with other scheduled jobs like Import which can fail to start.

### Procedure

---

Click Manage > Central Management > Portal User Sync to manage portal user synchronization.

- a. Click Modify Schedule to change the user synchronization task schedule by using the standard task scheduler.
- b. If the task is actively scheduled, click Pause to stop further scheduled executions.
- c. If the task is paused, click Resume to start running the task again (according to the defined schedule).

d. Click Run Once Now to run the synchronization task immediately.

Note: The task that is scheduled or Run Once Now refers to the collection of data and its transmission to the managed units only. The managed units might not use that data to update their user tables until up to 1 hour after it is received.

Restriction: The Central Manager and managed units must have the same SSH port for Portal User Sync to work. Use this CLI command to get the SSH port: `show ssh port`.

## Implementing Central Management in an Existing Installation

Implement Central Management in an existing Guardium environment and migrate a CAS collector with active instances to be managed.

In an existing Guardium environment, refer to the procedure outlined to develop a plan for implementing central management. If you are converting an existing Guardium unit to a Central Manager, keep in mind that a Central Manager cannot monitor network traffic. For example, inspection engines cannot be defined on a Central Manager.

1. Select a system shared secret to be used by the Central Manager and all managed units. For more information, see the system shared secret in System Configuration.
2. Install the Central Manager unit or designate one of the existing systems as the Central Manager. In either case, use the store unit type command to set the manager attribute for the Central Manager.
3. Any definitions from the stand-alone unit that you want to have available in the central management environment must be exported before the stand-alone unit is registered for management. Later, those definitions are imported on the Central Manager. BEFORE exporting or importing any definitions, follow the procedure that is outlined for each stand-alone unit that is to become a managed unit. Read through the introductory information under Export/Import Definitions.
  - Decide which definitions from the standalone system you want to have available after the system becomes a managed unit. Ignore any components on the stand-alone system you do not want to have available.
  - Compare the security roles and groups that are defined on the stand-alone unit with those defined on the Central Manager. Under central management, a single version of these definitions applies to all units. If a security role with the same name exists on both systems and it is used for different purposes, add a new role on the Central Manager and assign the new role to the appropriate definitions after they are imported.
  - If the same group name exists on the stand-alone unit and the Central Manager but it has different members, create a new duplicate group on the stand-alone system, taking care to select a group name that does not exist on the Central Manager. In all of the definitions to be exported, change the old group name references to new group name references.
  - All security roles that are assigned to all definitions that are exported from the stand-alone system. When definitions are imported, they are imported WITHOUT roles, so you must add them manually.
  - Check the application role permissions on each system. If any security roles assigned to an application on the stand-alone unit are missing from the Central Manager, add them to the Central Manager.
  - Export all definitions from the stand-alone system that you want to have available after the system becomes a managed unit. (See Export/Import Definitions) Do not export users or security roles. If you are unsure about a definition, export it in a separate export operation so that you can decide in the future whether to import that definition to the Central Manager. After you register for central management, none of the old definitions from the stand-alone unit are available.
  - On the stand-alone unit, create PDF versions audit process results and store them in an appropriate location. Under central management, only the audit results produced under central management are available.
  - On the stand-alone unit, instruct all users to remove all portlets that contain custom report, and to not create any new reports until the conversion to central management is complete.
  - On the Central Manager, manually add all users from the stand-alone unit.
  - On the stand-alone unit, delete all user definitions except for the admin user (which cannot be deleted).
  - Register the stand-alone unit for central management. See Registering Units for Central Management.
  - On the Central Manager, import all definitions that are exported from the stand-alone system. Check to make sure that references to included items (receivers in alert notifications, for example) are correct. Reassign security roles, as necessary, to all imported definitions.
  - Inform users of the managed unit that they must use the Report Builder application to regenerate the portlets for any custom reports they want to display in their layouts.

## Migrating a stand-alone CAS collector to managed

Use the following steps when you migrate a CAS collector with active instances to managed.

1. Export the CAS host definitions from the stand-alone collector.
2. Manage the stand-alone collector.
3. Restart the CAS host from the GUI of the now managed collector.
4. Import the CAS host definition to the manager.
5. Restart the CAS host from the GUI of the managed collector again.

After these steps are performed, the CAS collector has the same instances and monitor the same files that it did when it was a stand-alone.

Note: The CAS data that was collected when it was a standalone is deleted. There is no collected CAS data unless a file changes.

## Using Central Management Functions

Use Central Management functions to synchronize portal user accounts, monitor managed units, and install security policies on managed units.

- **[Managing expiring certificates](#)**  
12.1 and later You can view, manage, update, and distribute certificates from Guardium Data Protection central manager to the central manager and the managed units.
- **[Deployment health views](#)**  
The deployment health views gather and display information about your entire Guardium environment in powerful, easily consumed graphical views.
- **[Creating a cross-CM health view](#)**  
The cross-central manager health view (cross-CM health view) is a Guardium unit type that provides aggregated health views for an entire Guardium deployment.

These views include health information for all available central managers, aggregators, collectors, and S-TAPs in your environment. After you build a cross-CM health view unit, you can manage patches for all the central managers that are associated with that unit.

- **S-TAP and GIM dashboard**

This dashboard presents S-TAP and GIM health, status, version, and other information through several easy-to-use charts.

- **Create and manage S-TAP clusters**

Learn how to define S-TAP clusters in Guardium that are useful for managing active-passive S-TAP cluster arrangements on your data servers.

- **Enterprise load balancing**

The enterprise load balancer dynamically allocates managed units to S-TAP agents based on system load and availability.

- **Deployment inventory**

The inventory view provides centralized view of all database servers and any installed S-TAPs or GIM clients.

- **Resource deployment view**

The resource deployment view shows the GIM clients and S-TAPs installed on the database servers in a Guardium environment.

- **Monitoring managed units**

Monitor managed units from the Guardium Central Management page.

- **Creating managed unit groups**

Organize managed units into groups and then take actions on those groups.

- **Installing security policies on managed units**

Install a security policy on a manage unit.

- **Central patch management**

Provide visibility and control over patch installation, status, and history.

- **Distributing authentication configuration**

Instead of configuring authentication on each appliance separately, central management authentication (Configure Authentication) can be configured once on the central manager and then distributed to all managed units. This way, information is entered once and it applies to some or all units; some of the units may have a different type of authentication.

- **Distributing configurations**

Configurations and their schedules, can be distributed, either all or individually, between the central manager and the managed units.

- **Working with configuration profiles**

Configuration profiles allow you to define configuration and scheduling settings from a central manager and distribute those settings to managed unit groups without altering the configuration of the central manager itself.

- **Distribute custom tables**

Distribute custom tables and their data from a central manager to managed units.

- **Central manager redundancy**

Use Central Manager Redundancy or Backup Central Manager (CM) to configure a secondary or backup CM in case the Primary CM becomes unavailable.

---

## Managing expiring certificates

12.1 and later You can view, manage, update, and distribute certificates from Guardium® Data Protection central manager to the central manager and the managed units.

### About this task

For nontrusted certificates, you can distribute only the certificates that are issued from externally generated certificate signing requests (CSRs); these certificates need a private key and server certificate.

Note: You cannot distribute MySQL and GIM certificates from Guardium Data Protection central manager to the managed units.

You can distribute certificates from the central manager to managed units that are 12.1 or later only.

### Procedure

1. From the Manage menu, browse to System View > Certificate Management.

2. From the list, select the certificate that you want to update.

The different colors indicate the time period of expiry. For example, red color indicates that the certificate has expired and orange color indicates that the certificate expires in less than 180 days.

Note: You cannot update the self-signed certificates such as `keystore_default`, and patch certificates such as `patch-signing.cert.pem`.

3. Click Update certificate. The Update certificate window is displayed.

4. Paste the newly signed certificate.

- If you are using public certificates, paste the newly signed certificate.
- If you are using server certificates like Tomcat, paste the private key, server certificate, intermediate key, and the root certificate.

Note: Make sure to paste the correct certificate information in the text box.

5. All the units to which the updated certificate is applicable are selected by default. If you do not want the certificate to be distributed to a unit, clear the checkbox.

Note: If a managed unit is not accessible from the central manager, the updated certificates are not distributed to that managed unit.

6. Select the Restart Tomcat on the units after update checkbox if you want to restart Tomcat on the managed units after the certificates are updated.

7. Click Update. A window displays the success message, and the location of the log file to view the update.

### Results

The certificate distribution occurs in the background. You can monitor the progress of the certificate update in the log file `dist_certificate.log`.

Note: You cannot view the progress of the certificate distribution in the GUI.

You can also monitor the progress by using the `distribute_certificate showlog` CLI command.

---

## Deployment health views

The deployment health views gather and display information about your entire Guardium® environment in powerful, easily consumed graphical views.

The deployment health views help you investigate system-utilization trends and quickly identify ailing or down systems. These views decrease reaction times and reduce risks from problems in your Guardium deployment. The deployment health views are designed to work together by consolidating several different sources of information into unique but related views.

#### Deployment health topology and table views

The deployment health topology and table views show the data flow relationships between systems in your environment. These views make it easy to identify problematic systems and investigate the underlying issues.

- To access the topology view, browse to [Manage > System View > Deployment Health Topology](#).
- To access the table view, browse to [Manage > System View > Deployment Health Table](#).

#### Deployment health dashboard

The deployment health dashboard provides an at-a-glance summary of issues that are found across a Guardium deployment. The dashboard is especially useful for identifying patterns and trends in the health data before investigating individual systems where problems are identified.

To access the dashboard, browse to [Manage > System View > Deployment Health Dashboard](#).

The following table summarizes the types of data available to each of the deployment health views.

Table 1. Summary of deployment health views

|                                              | Dashboard | Topology | Table |
|----------------------------------------------|-----------|----------|-------|
| Unit utilization                             | ✓         | ✓        | ✓     |
| Correlation alerts                           | ✓         |          |       |
| Self-monitoring                              | ✓         |          |       |
| System requirements                          | ✓         |          |       |
| Aggregation                                  |           | ✓        | ✓     |
| Inspection engines (S-TAP verification data) |           | ✓        |       |
| Connectivity                                 |           | ✓        | ✓     |
| S-TAP connectivity                           |           | ✓        |       |

Attention: The deployment health views present data gathered from an entire Guardium environment and are only available from a central manager.

- [\*\*Configuring a central manager for the deployment health views\*\*](#)

To use the deployment health views, enable the collection of unit utilization data, configure correlation alerts, and configure data import and export for your environment.

- [\*\*Deployment health topology and table views\*\*](#)

Learn more about how the deployment health topology and table views present the configuration of your Guardium environment and its data.

- [\*\*Deployment health dashboard\*\*](#)

Learn more about how the deployment health dashboard presents data from your entire Guardium deployment.

- [\*\*Scenario: Troubleshooting overloaded systems using the deployment health topology view\*\*](#)

This topic describes using the deployment health topology view to identify and fix an overloaded system in your environment.

## Configuring a central manager for the deployment health views

To use the deployment health views, enable the collection of unit utilization data, configure correlation alerts, and configure data import and export for your environment.

### About this task

From a central manager, the deployment health views display data from across a Guardium® environment. The ability to display data about an entire deployment requires the collection of unit utilization data, the configuration of correlation alerts, and that data import, export, and S-TAP verification is correctly configured. For a summary of data that is displayed on the deployment health views, see [Deployment health views](#).

It is likely that your deployment is already configured to support the deployment health views. Verify the configuration steps that are described in this procedure if you notice any of the following issues on any of the deployment health views:

- CM buffer usage report not scheduled
- Unit utilization report not scheduled
- Export not scheduled
- Import not scheduled
- No issues found
- Status unavailable

The S-TAP details include the inspection engines and their database versions if the auto-discovery feature is enabled. On Unix-Linux databases, auto-discovery is enabled by default and runs once daily. For more details, see [Linux-Unix: Discover database instances](#). On Windows databases, auto-discovery is not enabled by default because it would overwrite user modifications to the inspection engine configurations. For more details, see [Windows: Discover database instances](#)

### Procedure

1. Configure the collection and processing of unit utilization data from the central manager.

For more information, see [Configuring unit utilization data processing](#).

2. Enable correlation alerts for inclusion on the deployment health dashboard.

a. Open [Protect > Database Intrusion Protection > Alert Builder](#).

b. Select an existing alert and click the icon, or create a new alert by clicking the icon.

c. Provide a Category for the alert.

Alerts without a specified category are displayed as Uncategorized.

d. Select the View in deployment health dashboard checkbox to include the alert on the dashboard.

Attention: Alerts must have the Severity set to LOW, MED, or HIGH to be included on the deployment health dashboard.

For more information about defining alerts, see [Building alerts](#).

### 3. Configure data import and export from the central manager.

For more information, see [Data aggregation](#).

Tip: Use the distribute configuration profiles tool to simplify the process of configuring data import and export for a Guardium deployment. For more information, see [Working with configuration profiles](#).

### 4. Configure S-TAP verification for all supported S-TAPs.

For more information, see [Windows Inspection engine verification](#) and [Linux-UNIX Inspection engine verification](#).

## Results

---

After you complete the configuration procedures and allow the data to update, the deployment health topology and deployment health table views predominately show  status except for systems with preexisting health issues. The deployment health dashboard includes any preexisting unit utilization issues and begins showing new correlation alert conditions.

After altering the unit utilization or data import and export schedules, wait up to 1 hour to allow the deployment health views to update with new information. The availability of new correlation alert data depends on the notification frequency that is specified for an alert.

## Related concepts

---

- [Data aggregation](#)
- [Correlation Alerts](#)

## Related tasks

---

- [Configuring unit utilization data processing](#)
- [Working with configuration profiles](#)

## Deployment health topology and table views

---

Learn more about how the deployment health topology and table views present the configuration of your Guardium® environment and its data.

The deployment health topology view is accessible from any central manager and provides an at-a-glance visualization of the entire Guardium environment that is connected to that central manager. In addition to showing relationships between nodes in the environment, the deployment health topology view also provides health information about all connected aggregators, collectors, and S-TAPs. Several investigation and resolution actions are available directly from the deployment health topology view to help quickly address health issues that are discovered in your environment.

Tip: It is also possible to view aggregated health data from across multiple central managers by establishing a cross-CM *health* view system in your environment. For more information, see [Viewing cross-CM health view deployment health data](#).

The default deployment health topology view is a data flow view that shows the data import and export relationships between aggregators and managed units. Browse to the deployment health topology view at [Manage > System View > Deployment Health Topology](#).

A sortable table view of the deployment health data is also available at [Manage > System View > Deployment Health Table](#). In the table view, the Guardium systems tab provides overall deployment health information while the S-TAPs tab provides detailed health information about S-TAPs and databases.

## Data availability

---

Several factors influence that availability of system data and how that data is displayed on the deployment health topology and table views. For information about configuring your system to use the deployment health views, see [Configuring a central manager for the deployment health views](#).

The backup central manager only shows its connectivity status.

### Types of data

When correctly configured, the deployment health topology and table views display data that is collected from several different sources. The specific types of data that are displayed depend on the unit type, as summarized in the following sections.

#### Overall Status

The overall status gives the status of the unit:

- Overall status.
- Guardium version for Guardium systems and S-TAPs.
- OS version, databases, and database status for S-TAPs, including S-TAP type, version, and verification status. For more information, see [Windows: Inspection engine verification / Linux-UNIX: Inspection engine verification](#).

#### Connectivity

The connectivity category indicates whether systems in a Guardium environment are able to communicate.

- Applies to central managers, aggregators, collectors, and S-TAPs.
- Examples include unit not responding and S-TAP not responding, and incorrect S-TAP configuration.

#### Investigation dashboard

The investigation dashboard category indicates whether there are open issues with the investigation dashboard environment.

- Applies to central managers, aggregators, and collectors.
- For more information see [Investigation dashboard issues](#).

#### 12.1 and later Monitored processes

This report provides combined information about the Investigation dashboard and Threshold alerter.

- **Investigation dashboard**

The investigation dashboard category indicates whether there are open issues with the investigation dashboard environment.

- Applies to central managers, aggregators, and collectors.
- For more information see [Investigation dashboard issues](#).

- **Threshold alerter**

The threshold alerter category indicates whether the alerter service is down.

- Applies to central managers, aggregators and collector.

#### View Unit utilization report

This report provides information about how heavily Guardium systems are loaded.

- Applies to central managers, aggregators, and collectors.
- Examples include CPU load, free buffer space, and MySQL disk usage.
- For more information, see [Unit utilization and inspection core performance](#).

#### View Aggregation/Archive Log

This log provides information about data import and export flow between Guardium systems.

- Applies to central managers (if configured as aggregators), aggregators, and collectors.
- Examples include import failed, export failed, and export not scheduled.
- For more information, see [Predefined admin reports](#) and [Data aggregation](#).

#### S-TAP only

##### K-TAP status

The K-TAP status indicates whether K-TAP is successfully loaded. Use the View S-TAP events link for more information.

##### Traffic status

If Traffic is selected from the Customize settings menu, then Guardium checks the status of traffic between S-TAPs and Guardium.

- Applies to central managers, aggregators, and collectors.
- For topology views, traffic status displays on the S-TAP roll-up.
- By default, traffic is queried every five minutes on the collector, but you can modify this interval (to between 5 and 30 minutes) with the `set_health_traffic_job_interval` API. If the status changes, the data is pushed to the central manager every 5 minutes. In most cases, traffic data is less than 10 minutes old (but can be as much as 20 minutes old in some worst-case scenarios).

##### Data latency

Several preset and user-defined schedules determine the latency of data that is displayed on the deployment health topology view. These schedules are summarized in the following table.

Table 1. Deployment health topology view data latency

| Health category         | Node type                                  | Latency                                                                                                                                       |
|-------------------------|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Connectivity            | Aggregator or collector                    | Less than 15 minutes                                                                                                                          |
| Connectivity            | S-TAP, data stream, or universal connector | Less than 15 minutes if enterprise load balancing is enabled<br>Less than 1 hour if enterprise load balancing is not enabled                  |
| Aggregation             | Central manager, aggregator, or collector  | Less than 1 hour                                                                                                                              |
| Verification            | S-TAP                                      | Less than 1 hour                                                                                                                              |
| Unit utilization        | Central manager, aggregator, or collector  | 1 - 2 hours, based on the recommended configuration. For more information, see <a href="#">Configuring unit utilization data processing</a> . |
| Investigation dashboard | Central manager, aggregator, or collector  | Less than 1 hour                                                                                                                              |

Observe the following latencies for specific environment and configuration changes:

- Newly registered aggregators or collectors become available to the deployment health views within 15 minutes.
- Deleting the data export schedule or data export configuration from a collector are reflected on the deployment health views within 2 hours.

## Data presentation

##### Health status

The deployment health topology view displays three categories of health information for Guardium systems: connectivity, unit utilization, and aggregation. Metrics under these categories are assigned one of the following health statuses: status unavailable (least severe), no health issues, low severity, medium severity, and high severity (most severe). The overall status is determined by the most severe status of any individual metric included under any of the health categories being displayed. Data that has been excluded using the Customize Settings dialog is not used for determining the overall status of a system.

For example, if the Restarts metric under the Unit utilization category is assigned a High severity status, but no health issues exist under another category, the Overall status for that system is High severity. This behavior ensures that the most severe condition is always visible at-a-glance as the overall status of a system.

At the Manage > System View > Deployment Health Topology view, detailed statuses for the available health categories are only displayed when at least one low, medium, or high severity issue is found.

At the Manage > System View > Deployment Health Table view, detailed statuses for the available health categories are always displayed.

##### Health status roll-up

The deployment health topology view implements a health status roll-up strategy to efficiently display health information for an entire Guardium environment. Using this strategy, child nodes are collapsed under their parent nodes, and the child's health status is rolled-up to the parent. The rolled-up status is expressed as a small icon attached to the parent node.

Attention: Health status roll-up is only supported for S-TAP nodes rolling-up status to their parent collector.

For example,  indicates a collector with no health issues, but the small red circle indicates that one or more S-TAPs that are associated with that collector has high severity issues. Clicking the collector expands the node and reveals the associated S-TAPs and their health status. For example,



indicates four S-TAPs that are associated with the collector: two S-TAPs have high severity health issues, and two S-TAPs have low severity health issues. Only the most severe status is rolled-up from the child to the parent node when the child nodes are collapsed. In the previous example, the parent node shows a small red circle because one or more of its children has high severity issues. However, if one or more child nodes contain low severity issues but all the other child nodes have no health issues, the parent node would display a small yellow circle.

#### Filtering

The topology view provides Active filters for several metrics, such as database type, host name, and health severity. Use the filter-type fields to select and apply filters to the topology.

The table view provides quick filtering by health status using the Filter overall status by check boxes in the table header. In addition to quick filtering, the table view also provides Advanced filter controls that can be configured and saved.

1. Use the icon to open the Advanced filter pane.
2. To use an existing filter, select one from the Saved filters menu and click Apply Filter.
3. To create a new filter:
  - a. Leave the Saved filter field blank.
  - b. Use the menus and fields to define filtering criteria.
  - c. Click Save.
  - d. On the Save Filter dialog, use the Filter name field to name the filter.
  - e. Click Save and Apply or Save Filter.
4. Use the Remove link in the table header to disable an advance filter that has been applied.

#### Customizing the settings

Click the icon to open the Customize Settings dialog and define the following properties:

- From the Health Settings tab:
  - The health status categories to display, such as connectivity, traffic, and unit utilization.
  - Display settings for the topology view, such as default zoom settings, and whether to exclude healthy nodes or expand S-TAPs by default.
  - Column-display settings for the table view.
  - Other settings, such as whether to show S-TAP aliases.
- From the Traffic ignore list tab, you can select one or more databases to ignore for traffic monitoring. If you do not select Traffic from the Health Settings tab, traffic is not monitored.
  1. From the Traffic ignore list tab, click the icon to display a list of all available databases.
  2. Select the databases to ignore. You might, for example, want to ignore test databases.
  3. Click Add to ignore list.

## Deployment presentation

Some deployment configurations display unexpectedly on the deployment health topology view. Several of these configuration scenarios are described in the following sections.

#### Unsupported S-TAPs

The deployment health topology view displays any S-TAPs that are configured for S-TAP verification or that participate in enterprise load balancing. If an S-TAP cannot be configured for S-TAP verification or to participate in enterprise load balancing, it is not displayed.

#### S-TAP load balancing

If S-TAP load balancing is configured with the `participate_in_load_balancing` parameter and an S-TAP is configured to balance traffic across multiple collectors, the deployment health topology view displays that S-TAP as a child node of each collector. For example, if S-TAP 1 is load balancing with *Collector A* and *Collector B*, both *Collector A* and *Collector B* display S-TAP 1 as a child in the deployment health topology view.

#### Invalid S-TAPs

Invalid S-TAPs are similar to inactive S-TAPs, but they only appear in topology views. Use the API [delete\\_invalid\\_stap](#) to remove invalid S-TAPs from the topology views.

#### Unmanaged units

If a collector exports data to a central manager or to an aggregator that is configured as a central manager, but that collector is not designated as a managed unit of that central management cluster, the Overall status of the collector in the deployment health topology view is shown as Health status unavailable. No additional information about the collector is made available through the deployment health topology view unless the collector is designated as a managed unit of the central manager.

#### Collector exporting data to primary and secondary hosts

When a collector is configured to export data to both primary and secondary hosts, only the primary host is used for the deployment health topology view.

## Related tasks

- [Configuring a central manager for the deployment health views](#)

## Deployment health dashboard

Learn more about how the deployment health dashboard presents data from your entire Guardium® deployment.

## Data availability

Several factors influence the availability and latency of health data and how that data is displayed on the deployment health dashboard. The following table summarizes the data included on the dashboard, trigger criteria, and data latency and purge information.

Table 1. Summary of deployment health dashboard data

| Data source            | Information type                                                                       | Trigger criteria                                                                             | Data latency                                                                                                                                                                                                                                                                                                                                                                                | Data purge interval                                                                                    |
|------------------------|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Analyze limits         | Information such as MySQL connections, HTTP GUI connections, and Tomcat open handlers. | Not applicable                                                                               | Updated every 5 - 10 minutes.<br><br>The purge interval is configurable using the CLI command <b>store purge object age</b>                                                                                                                                                                                                                                                                 | Data is purged after 14 days<br><br>Data is purged after 7 days                                        |
| Correlation alerts     | Triggered correlation alerts                                                           | An alert threshold is reached                                                                | Updated based on the alert notification frequency. For more information, see <a href="#">Correlation Alerts</a> .                                                                                                                                                                                                                                                                           | Data is purged after 7 days                                                                            |
| System resources       | System configuration, such as CPU cores, system memory, /var disk capacity             | System does not meet minimum requirements                                                    | Updated whenever the user-interface server is started or restarted                                                                                                                                                                                                                                                                                                                          | Not applicable                                                                                         |
| System self-monitoring | MySQL disk usage and system disk usage                                                 | Usage meets or exceeds default thresholds (75% for high severity, 90% for critical severity) | Updated every 5 - 10 minutes.<br><br>For high-severity, if the same event occurs multiple times in a 15 minute period, the timestamp is updated to reflect the most recent instance. If the same event occurs after a 15 minute interval, a new entry is created with the most recent timestamp.<br><br>For critical issues, every instance of an event is created with a unique timestamp. | High-severity issues are purged after 7 days<br><br>Critical issues are never purged                   |
| Unit utilization       | Unit utilization data such as sniffer restarts, MySQL disk usage, and CPU load.        | Value exceeds unit utilization thresholds                                                    | Updated within 1 - 2 hours, based on the recommended configuration. For more information, see <a href="#">Configuring unit utilization data processing</a> .                                                                                                                                                                                                                                | Unit utilization data is purged after 60 days<br><br>Sniffer buffer usage data is purged after 14 days |

Important:

- Only data from systems that are running Guardium V10.1.2 and later are included on the deployment health dashboard.
- When you change the host name of a system, preexisting data that is associated with the original host name is no longer displayed on the deployment health dashboard.
- When a primary central manager transfers data to a backup central manager during a failover scenario, up to 30 minutes of data is unavailable to the deployment health dashboard.

## Data presentation

The deployment health dashboard formats and presents data through various tiles or small window-like containers. The following table summarizes the data that is presented on each dashboard tile.

Table 2. Summary of deployment health dashboard tiles

| Data source            | Tile name                                               |                        |                         |                             |                                                 |        |                                               |                                               |
|------------------------|---------------------------------------------------------|------------------------|-------------------------|-----------------------------|-------------------------------------------------|--------|-----------------------------------------------|-----------------------------------------------|
|                        | Resource requirements                                   | Central manager limits | Unit utilization issues | Unit utilization timecharts | Alerts (by category, name, severity, or system) | Events | High severity                                 | Critical                                      |
| Analyze data           | ✓ (values are a percentage of user-configurable limits) |                        |                         |                             |                                                 |        |                                               |                                               |
| Correlation alerts     |                                                         |                        |                         |                             | ✓                                               | ✓      | ✓                                             |                                               |
| System resources       | ✓                                                       |                        |                         |                             |                                                 |        | ✓                                             |                                               |
| System self-monitoring |                                                         |                        |                         |                             |                                                 | ✓      | ✓ (When usage meets or exceeds 75% threshold) | ✓ (When usage meets or exceeds 90% threshold) |
| Unit utilization       |                                                         |                        | ✓                       | ✓                           |                                                 | ✓      | ✓                                             |                                               |

The following tiles are displayed by default: *alerts by name*, *central manager limits*, *critical issues*, *events timeline*, *high severity issues*, and *unit utilization issues*.

## Dashboard filter

The dashboard filter allows quick filtering of the data based on Guardium systems, issue severity, and time period. Filter settings affect the data displayed on the entire dashboard unless noted otherwise.

The Guardium systems filter allows filtering the dashboard by unit type or by groups defined at [Manage > Central Management > Managed Unit Groups](#).

By default, the dashboard displays all available issues: low, medium, high, and critical. Use the Severity menu to filter data on the dashboard by severity. Selecting high filters the entire dashboard to display only high-severity issues. Selecting critical filters the entire dashboard to display only critical issues. It is possible to select both high and critical issues to filter out all lower-severity data.

Notes:

- Outstanding or unresolved critical issues are displayed on the dashboard regardless of the Severity filter setting.
- For the *unit utilization issues* tile, the dashboard Severity filter is based on the overall unit utilization severity. For more information about how unit utilization severity is assigned, see [Unit utilization issues](#).

The time filter determines the range of data that is displayed on the dashboard. Default settings allow time periods from 1 hour to 3 weeks, but custom time periods are also supported. The time filter does not apply to critical issues: critical issues are always displayed, regardless of the time filter setting.

Use the Add chart menu to add tiles to the dashboard or replace default tiles that you previously removed.

## Dashboard summary

The dashboard summary provides overall counts of health issues that are detected in your Guardium deployment. The Collectors with issues and Aggregators with issues counts indicate the number of systems--collectors and aggregators--that are detected with health issues. The Critical and High counts indicate the number of issues detected from all systems that are included on the dashboard.

Note:

- The Critical and High counts are not affected by adding or removing tiles from the dashboard.
- The counts on the dashboard summary bar reflect the dashboard filter settings.

## Alerts by category, name, severity, or system

The deployment health dashboard supports several tiles based on Guardium correlation alerts: *Alerts by category*, *Alerts by name*, *Alerts by severity*, and *Alerts by system*. Add correlation alert tiles to the dashboard by using the Add chart menu.

Correlation alerts must be explicitly configured for inclusion on the deployment health dashboard. For information about configuring alerts for the dashboard, see [Configuring a central manager for the deployment health views](#).

## Central manager limits

The *central manager limits* tile displays information to help assess central manager activity over time. For example, *MySQL connections*, *HTTP GUI connections*, *Tomcat open handlers*, and other related metrics are tracked on the tile.

All values are expressed as a percentage of a defined *analyze limit* threshold. For example, if a threshold is set at 80%, the tile indicates 100% when that 80% threshold is reached. The thresholds are configurable using the **modify\_guard\_param** API command. For more information, see the *analyze limits parameters* section of [modify.guard.param](#).

Customize the tile to include or exclude specific metrics and show or hide the legend.

## Resource requirements

The *resource requirements* tile indicates whether systems in a Guardium deployment meet the minimum hardware requirements for CPU, memory, and /var disk capacity. Any system resource that does not meet the minimum requirement is designated as a high-severity issue and displayed on both the *resource requirements* tile and the *high severity issues* tile.

Use the Include healthy systems check box on the details view of the tile to include all available data for the systems and time frame that are indicated on the dashboard filter bar. By including all available data, the Include healthy systems check box overrides the Severity setting of the overall dashboard filter. Systems without any detected health issues are excluded by default.

A table that displays all met and unmet resource requirements in your Guardium deployment is also available at Manage > Central Management > System Resources. Note:

- System resource issues are not displayed in the *Events* timeline because they are not associated with a specific time stamp

## Unit utilization issues

The *unit utilization issues* tile displays issues based on unit utilization thresholds. The issues that are displayed on the tile represent individual metrics that exceed their respective thresholds. The overall severity is assigned based on the highest severity issue that is found in all available metrics for an individual system in a specified time period. For more information about unit utilization thresholds, see [Unit utilization and inspection core performance](#).

The details view of the *unit utilization issues* tile includes both a Period start time and a Timestamp:

- The Period start time indicates that the *CM buffer usage monitor* data is rolled-up into hourly periods, for example periods starting at 13:00, 12:00, and 11:00.
- The Timestamp indicates when the unit utilization levels data is added to the deployment health dashboard, either based on the unit utilization levels schedule or by using *run once now*.

For more information, see [Configuring unit utilization data processing](#).

The first time that unit utilization data is brought into the deployment health dashboard, all the unit utilization data has the same *timestamp* but different *period start* times. Over time, the time stamps will appear at intervals based on the unit utilization levels schedule. For example, if the unit utilization levels data is collected every hour at 40 minutes after the hour, you will see *period start time* and *timestamp* values as follows:

Table 3. Example unit utilization period start time and timestamp values

| Period start | Timestamp |
|--------------|-----------|
| 13:00        | 14:40     |
| 12:00        | 13:40     |
| 11:00        | 12:40     |

Use the Include healthy systems check box on the details view of the tile to include all available data for the systems and time frame that are indicated on the dashboard filter bar. By including all available data, the Include healthy systems check box overrides the Severity setting of the overall dashboard filter. Systems without any detected

health issues are excluded by default.

## Unit utilization timecharts

*Unit utilization timecharts* allow the observation of trends in unit utilization data over time. *Unit utilization timecharts* can be configured to show multiple unit utilization metrics for a single Guardium system or to show a single unit utilization metric for multiple Guardium systems.

*Unit utilization timecharts* are structured based on the following criteria:

- The x-axis represents the *period start* time
- When multiple metrics are being charted and the values for the metrics are in the same range, one y-axis is drawn. For example, both *MySQL disk usage* and */var disk usage* are expressed as percentages and are drawn with the same y-axis.
- When multiple metrics are being charted and the values of the metrics are not similar, two y-axes are drawn. For example, *MySQL disk usage* is expressed as a percentage and *flat log requests* is expressed as an integer, so two y-axes are drawn: one displaying percentages and one displaying integers.
- If the value of a metric falls outside the range of a y-axis, that value is displayed at the bottom of the chart. This behavior accommodates scenarios where different metrics are expressed with similar units but significantly different values: for example, integers in the range of thousands versus millions.

Tip: Create multiple time charts when values are in significantly different ranges.

Note: Systems are not included on Timechart settings Host name menu when unit utilization data does not exist for that system in the time frame that is specified on the dashboard filter bar.

## Related tasks

- [Configuring a central manager for the deployment health views](#)
- [Configuring unit utilization data processing](#)

## Scenario: Troubleshooting overloaded systems using the deployment health topology view

This topic describes using the deployment health topology view to identify and fix an overloaded system in your environment.

## About this task

This scenario involves identifying health issues from the deployment health topology view, assessing the root cause, and correlating that assessment with additional data before resolving the problem and verifying the fix. The example described here involves an overloaded collector, but the process is applicable for other cases.

## Procedure

1. On a central manager, navigate to Manage System View Deployment Health Topology.
2. Review the deployment topology and assess the overall health of systems in the environment.  
At a high level, icons indicate healthy systems while and icons indicate systems with some health issues.
3. If you notice systems with or status icons, click the node to view an overlay with additional health information.
4. Use the information presented on the node overlay to begin diagnosing any health problems. For example, a collector with high or medium severity statuses for */var disk usage*, *Restarts*, *Analyzer queue*, and *Logger queue* indicates that the collector is overloaded.
5. After initially assessing health issues from the deployment health topology view, try to correlate your findings with additional data. For example, if you suspect that a system is overloaded, begin monitoring the traffic for that system.
6. When you are confident that you have diagnosed the underlying health issues, take corrective actions. In the example of an overloaded system, you could establish [Enterprise load balancing](#) or reassign S-TAPs to another collector.  
Typically, this set of symptoms would not occur if enterprise load balancing was already configured and in use.
7. After taking corrective actions, the status of the node on the deployment health topology view will be updated following the next refresh of unit utilization and central manager buffer usage monitor data. This refresh interval depends on your [schedule for processing unit utilization data](#).

## Related information

- [S-TAP user's guide](#)

## Creating a cross-CM health view

The cross-central manager health view (cross-CM health view) is a Guardium unit type that provides aggregated health views for an entire Guardium deployment. These views include health information for all available central managers, aggregators, collectors, and S-TAPs in your environment. After you build a cross-CM health view unit, you can manage patches for all the central managers that are associated with that unit.

## Before you begin

Important: Build your cross-CM health view system as a new Guardium unit that is dedicated to viewing deployment health across your entire environment. Unlike a standard central manager, a cross-CM health view system is not intended for providing other types of data or managed functionality.

- Central managers registered to the cross-CM health view system must be at version 11.5p530 or later
- Communication over port 8443 between the cross-CM health view system and connected central managers

Note:

- If you have access to deployment health views on the cross-CM health view system, you can view health information for all Guardium units that are connected to the cross-CM health view system. However, you do not have any additional access to those connected systems beyond the access that their role provides.
- For user access and roles management, treat the cross-CM health view system as a stand-alone unit.
- When you upgrade Guardium systems in your environment, treat the cross-CM health view system as a stand-alone unit.

## About this task

---

### Procedure

---

1. Deploy a new Guardium aggregator. For more information, see [Installing your Guardium Data Protection system](#).
2. Change the system type to cross-CM health view by running the following CLI command:

```
store unit type cmhealthview
```

3. Register central managers to the cross-CM health view system by running the following API command:  
12.0 Syntax

```
grdapic modify_guard_param paramName=CM_HEALTH_VIEW_HOSTNAME paramValue=<host name of cross-CM health view system>
```

The preceding command registers 12.0 and earlier versions of central manager to the cross-CM health view system.

12.1 and later Syntax

```
grdapic register_unit unitIp="" unitPort="" secretKey=""
```

The preceding command registers 12.1 central manager to the cross-CM health view system.

- Run the command from each central manager that you are registering to the cross-CM health view system.
- The health data is forwarded from the central manager to the cross-CM health view system. No other types of data or managed functionality is provided.

Note:

12.0 You can unregister central managers from the cross-CM health view system by providing an empty `paramValue` for `CM_HEALTH_VIEW_HOSTNAME`.

Unregistered systems still appear on the aggregated health views of the cross-CM health view system, but their data is no longer updated and their status may not be listed accurately.

```
grdapic modify_guard_param paramName=CM_HEALTH_VIEW_HOSTNAME paramValue=
```

12.1 and later You can unregister 12.1 central manager from the cross-CM health view system by providing the central manager name.

```
grdapic unregister_unit unitIpList=""
```

### What to do next

---

After central managers are registered to the cross-CM health view system, you will begin seeing aggregated health data on the cross-CM health view system after a short delay. While the health data is being updated, the registered systems can indicate an *unknown* status and a *status updated* date from sometime in the past.

12.0 You cannot view the registered central managers in the Patch Management page.

12.1 and later You can manage patches and register and unregister central managers from the Patch Management page. You can also view the registered central managers in the Patch Management page. For more information, see [Managing patches on a cross-CM health view system](#).

- [Viewing cross-CM health view deployment health data](#)

After you create cross-central manager health view (cross-CM health view) Guardium unit, you can view aggregated health views for an entire Guardium deployment. These views include health information for all available central managers, aggregators, collectors, and S-TAPs in your environment.

- [Managing patches on a cross-CM health view system](#)

12.1 and later From the Patch Management UI on a cross-central manager health view (cross-CM health view) Guardium unit, you can view and update patches for multiple Guardium Data Protection central managers and their associated managed units.

## Viewing cross-CM health view deployment health data

---

After you create cross-central manager health view (cross-CM health view) Guardium unit, you can view aggregated health views for an entire Guardium deployment. These views include health information for all available central managers, aggregators, collectors, and S-TAPs in your environment.

The cross-CM health view system supports the following aggregated health views:

- Manage > System View > Deployment health topology
- Manage > System View > Deployment health table
- Manage > System View > S-TAP and GIM dashboard

These health views on a cross-CM health view system function as they do on a standard central manager but provide health data from multiple central managers. For more information about the deployment health views, see [Deployment health views](#). However, the following features (available on standard central managers) are not supported for a cross-CM health view system:

- Configuring the traffic ignore list
- The investigation dashboard status type

### Related concepts

---

- [Deployment health dashboard](#)
- [Deployment health topology and table views](#)

- [S-TAP and GIM dashboard](#)

## Managing patches on a cross-CM health view system

12.1 and later From the Patch Management UI on a cross-central manager health view (cross-CM health view) Guardium unit, you can view and update patches for multiple Guardium® Data Protection central managers and their associated managed units.

### Before you begin

Before you can view and manage available patches from the Patch Management page, you need to make them available to Guardium. For more information, see [Getting fixes from Fix Central](#) or [How to install patches](#).

To install patches on a central manager and its associated managed units, you must register the central manager on Patch Management. For more information, see [What to do next](#).

Note: Register (or reregister) all central managers that you want available for the deployment health view.

This feature is available on cross-CM health view systems only. You can install patches only on Guardium 12.1 and later central managers.

### Procedure

1. From a cross-CM health view unit, browse to System View > Patch Management.
2. From the CLI, run the following command to populate the Available patches table.

```
show system patch available
```

3. From Available patches, select the patch that you want to apply.

Note: You can select and install one patch at a time from the list.

4. From Registered units, select one or more units for which you want to apply the selected patch.

From the Registered units table, you can sort on any table column or filter on the following elements:

- Central manager name
- Managed unit group
- A search string

An admin user can assign roles to the central manager; only users with those assigned roles can access the central manager and their associated managed units and install the patch.

Note: Only the admin user that has access to the central manager can assign roles to the central manager.

5. Click Install to install the patch on all selected central managers.

6. In the Install Patch window, select a date if you want to schedule the patch installation, and then click Install

### What to do next

In addition to managing patches for your central managers, you can also register (and unregister) central manager units from the Patch Management window. To register a new unit, take the following steps:

1. From the Registered units table, click Register to open the Register New Unit window.
2. Enter the following information:
  - Unit IP - IP address (not the hostname) for the unit you want to register.
  - Unit port - The port for this unit. In general, use port 8443.
  - Secret access key - The system shared secret. For more information, see [Use the Same Shared Secret](#).
3. Click Register. After a few minutes, the unit is registered and is available in the Registered units table.

To unregister a unit, select the unit to unregister and click Unregister.

## S-TAP and GIM dashboard

This dashboard presents S-TAP and GIM health, status, version, and other information through several easy-to-use charts.

Data for the S-TAP and GIM dashboard is derived from the deployment health topology and table views. For more information, see [Deployment health views](#).

Open the dashboard at Manage > System View > S-TAP and GIM Dashboard.

The dashboard is divided into three sections:

#### S-TAP charts

Charts in this section support dynamic filtering: click on a chart element to filter the other charts by that element. For example, clicking Db2 on the Databases by inspection engine chart filters the other S-TAP charts so they only display information for S-TAPs with Db2 inspection engines. Use the Remove link to clear dynamic filters.

- S-TAP health summarizes S-TAP health status.
- S-TAPs by version shows how many S-TAPs are operating at specific version levels.
- Databases by inspection engine shows the different database types that are known in the environment.
- S-TAPs by operating system shows the different operating systems that are known in the environment. For Linux-UNIX operating systems, each distribution is represented by a vertical bar and the bars are segmented by version. For example, with two different versions of Red Hat Enterprise Linux (RHEL), the chart shows a single rhel bar divided into two segments (one for each version of RHEL). Similarly, one bar is used for Windows and the bar is segmented by version.
- S-TAPs with recent traffic. Use the Configure traffic metric link or use the icon and select the Traffic ignore list tab to create a list of hosts to exclude for the traffic metric. To exclude all traffic metrics for all hosts, use the icon and clear the Traffic check box on the Health settings tab.

Important: The list of hosts ignored for the traffic metric is shared between the S-TAP and GIM dashboard, the Deployment health topology, and the Deployment health table.

#### Historical charts

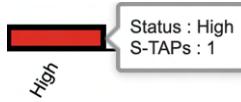
- S-TAP count shows the number of S-TAP that have detected traffic during the specified time period. Use the icon to set the time period.
- Inspection engine count shows the number of inspection engines that have detected traffic at 1-hour intervals for the past 3 hours. Use the icon to set the time period.

#### GIM charts

- GIM status summarizes the GIM client status information.
- GIM clients by version.
- S-TAP vs. GIM

Note: For S-TAPs or Guardium systems before V11.1, the operating system is listed only by the categories Linux-UNIX or Windows.

All charts are interactive such that hovering over a chart element shows details and tallies for that element. For example, hovering over a specific status bar in the S-TAP health chart shows the total number of S-TAPs with that status:



For each chart, use the icon to view a detailed table of the underlying data. The table views provide several troubleshooting features:

- Column sorting.
- Filtering using the Filter overall status by check boxes and the Filter text field.
- For S-TAP charts, view underlying inspection engines by expanding individual S-TAP rows.
- For S-TAP charts, investigate problems by selecting an individual S-TAP and using the Reports > S-TAP events report. If the S-TAP is associated with multiple collectors, each collector is shown in its own tab in the report.

This view can show invalid S-TAPs. Invalid S-TAPs are similar to inactive S-TAPs, but they only appear in some deployment health and deployment dashboard views. Use the **delete\_invalid\_stap** API command to remove invalid S-TAPs.

## Related reference

- [delete\\_invalid\\_stap](#)

## Create and manage S-TAP clusters

Learn how to define S-TAP clusters in Guardium that are useful for managing active-passive S-TAP cluster arrangements on your data servers.

## About this task

S-TAP clusters and the Manage S-TAP clusters page are only available on Guardium central managers.

## Procedure

1. Open Manage > System View > Manage S-TAP Clusters.  
The page displays a table of S-TAP clusters with standard , , and controls.
2. Create a new S-TAP cluster by clicking the icon to open the Add cluster dialog.
3. From the Cluster details tab of the Add cluster dialog:
  - a. Use the provided fields to enter a Cluster name, Cluster description, and Cluster IP.
  - b. Optional: Enable Remove inactive S-TAP connections by cluster.  
When enabled, this option automatically removes S-TAPs from Guardium when S-TAPs are not connected and the S-TAPs are part of an S-TAP cluster with one (and only one) connected S-TAP. If there are no active S-TAPs or multiple active S-TAPs in a cluster, no S-TAPs are removed from Guardium. Clusters are checked at a predefined interval.  
Important: When S-TAPs are removed using Remove inactive S-TAP connections by cluster, they are not merely removed from the S-TAP cluster: they are entirely removed from the Guardium system.
  - c. Optional: Enable Monitor S-TAP traffic by cluster.  
When enabled, this option changes how S-TAP traffic status is reported on the Deployment Health views: if one or more S-TAPs in the cluster has traffic, all S-TAPs in the cluster are reported as having traffic.
4. From the Cluster members tab of the Add cluster dialog, use the icon to add S-TAPs to the cluster.  
Manually enter an S-TAP IP address or host name, or use type-ahead functionality to select from existing S-TAPs.  
Note: S-TAPs may not be assigned to more than one S-TAP cluster.
5. Click Save to create the new S-TAP cluster.  
If Remove inactive S-TAP connections by cluster is enabled (see step 3.b), you are required to provide additional confirmation before continuing.

## Results

After creating S-TAP clusters, the Manage S-TAP Clusters table shows configuration summary for all S-TAP clusters. In addition:

- The Deployment health table includes an S-TAPs by cluster tab where you can review health information organized by S-TAP cluster.

- The Deployment health topology features S-TAP Cluster filters.
- The S-TAP and GIM Dashboard displays an S-TAP clusters with recent traffic tile.

## Enterprise load balancing

The enterprise load balancer dynamically allocates managed units to S-TAP agents based on system load and availability.

### Overview

Enterprise load balancing automates several tasks:

- It dynamically rebalances loaded or busy managed units by relocating S-TAP agents to managed units with lower loads. It balances the load of a group of S-TAPs among a group of managed units.
- It dynamically manages failover and unavailable managed unit scenarios, relocating S-TAP agents to another managed unit, or units, in its associated group.
- It evaluates the load of managed units before it assigns those managed units to an S-TAP agent.

See the Load Balancer Events report to review all load balancing activity.

Enterprise load balancing is disabled by default on Guardium® systems.

Enterprise load balancer does not balance the number of S-TAPs, sessions, or traffic. It allocates and moves S-TAPs between managed units to avoid overloading the sniffer process on those Guardium systems. The result is that some managed units have more S-TAPs pointing to them than others.

Note: S-TAP load balancing can be used simultaneously with enterprise load balancing, except for the grid model. For more details on S-TAP load balancing, see [Linux-UNIX: S-TAP load balancing models and configuration guidelines](#) and [Windows: S-TAP load balancing models and configuration guidelines](#).

### How it works

The enterprise load balancing application works by collecting and maintaining up-to-date load information from all its managed units. This process is called load collection.

It uses the load information to create a load map. This load map provides the data that directs load balancing and managed unit allocation activities. For more information, see [Viewing the enterprise load balancing load map](#).

Load collection errors from specific managed units are recorded in the Load Balancer Events report but do not interfere with the overall load collection and load balancing processes. However, failure to collect load information from a managed unit excludes that managed unit from participation in load balancing processes.

### Failover groups

If an S-TAP is requesting a new managed unit to fail over to, the load balancer searches in the associated managed unit group for an available managed unit. If it cannot find a managed unit, it continues its search in the failover groups until it finds one. You can define multiple failover groups.

You can prioritize the failover groups, for a controlled disaster recovery strategy. The load balancer searches for an available managed unit in the failover groups, starting with the group, or groups, whose priority is 1. Priority rule guidelines:

- The priority list must be sequential starting with 1.
- Multiple groups can have the same priority.
- The priorities cannot skip a level. For example, 1,1,2,3 is valid. However, 1,2,4,5 is invalid.

You must specify at least one associated managed unit group before you can specify a failover group association.

Attention: Make sure that all failover groups send their data to the same aggregator to simplify aggregation. (An exception is if you are using a data mart.) Load is not rebalanced within any one failover group.

- [Enabling enterprise load balancing and associating an S-TAP with a central manager](#)

First, enable enterprise load balancing on the central manager. Then, configure S-TAPs to point to the central manager. Then the central manager allocates managed units to the S-TAP.

- [Associating an S-TAP group with a managed units group for enterprise load balancing](#)

Learn how to use enterprise load balancing by creating and associating S-TAP groups with managed unit groups. If a managed group unit becomes unavailable, the S-TAPs sending data to that managed unit group are reassigned to the managed unit in the associated group with the lowest load. Optionally, define failover groups. You can specify multiple failover groups, with priorities, for disaster recovery.

- [Restarting \(resynchronizing\) S-TAPs for enterprise load balancing](#)

S-TAPs can become unsynchronized for a few reasons, for example, after you modify the S-TAP groups or the managed user groups in your centrally managed environment.

- [Viewing the enterprise load balancing load map](#)

Learn how to view the current enterprise load balancer load map.

- [Viewing an enterprise load balancing activity report](#)

View a report of enterprise load balancing events and activities.

- [Enterprise load balancing configuration parameters](#)

Use the load balancer configuration parameters to manage enterprise load balancing. To access the load balancing properties in a central manager, go to Manage > Central Management > Enterprise Load Balance > Enterprise Load Balance Properties. In a managed unit, go to Setup > Central Management > Registration and Load Balance.

## Enabling enterprise load balancing and associating an S-TAP with a central manager

First, enable enterprise load balancing on the central manager. Then, configure S-TAPs to point to the central manager. Then the central manager allocates managed units to the S-TAP.

## Before you begin

- The enterprise load balancer runs on a central manager or managed unit, listens to port 8443, and uses Transport Layer Security (TLS).
- No new firewall or extra system setup is required.
- Load information is only collected from managed units that are online and configured with the central management parameter LOAD\_BALANCER\_ENABLED=1. Setting LOAD\_BALANCER\_ENABLED=0 disables load balancing and prevents that managed unit from being dynamically allocated to S-TAP agents during load balancing activities.

## Procedure

1. Enable enterprise load balancing on the central manager. Go to [Manage > Central Management > Enterprise Load Balance > Enterprise Load Balance Properties](#) and set LOAD\_BALANCER\_ENABLED=1.
2. Point one or more S-TAPs to the central manager by modifying the S-TAP parameter in the S-TAP Control page:
  - Load balancer host name or IP address
  - load\_balancer\_port
3. Modify the S-TAP configuration parameters in the S-TAP Control page:
  - Managed Units: The number of managed units the enterprise load balancer allocates for this S-TAP.
  - Load balancing: Defines how the load is split between the assigned managed units. For example,
    - Managed Units=2, and Load balancing=1 (load balancing). The Enterprise Load Balancer assigns two managed units to the S-TAP, and traffic is split between the managed units.
    - Managed Units=2, and Load balancing=2 (mirroring). The Enterprise Load Balancer assigns two managed units to the S-TAP, and traffic is mirrored to both of the managed units.
  - For Unix-Linux databases only. Load balancer node affinity: Whether the S-TAP connects to more than one managed unit, for enterprise load balancing. Some scenarios need all traffic to go to the same collector. With Oracle ATAP, for example, the analyzed client IP only shows if both the encrypted and unencrypted sessions go to the same managed unit. For more information, see [Load balancer node affinity](#).

## What to do next

[Associating an S-TAP group with a managed units group for enterprise load balancing](#)

## Related concepts

- [Windows: S-TAP Control: Details](#)

## Related reference

- [Linux-UNIX: S-TAP Control: Details](#)

## Associating an S-TAP group with a managed units group for enterprise load balancing

Learn how to use enterprise load balancing by creating and associating S-TAP groups with managed unit groups. If a managed group unit becomes unavailable, the S-TAPs sending data to that managed unit group are reassigned to the managed unit in the associated group with the lowest load. Optionally, define failover groups. You can specify multiple failover groups, with priorities, for disaster recovery.

## About this task

When you specify multiple failover groups, each one has a priority. When the load balancer searches for an available managed unit in a failover group, it starts with the group, or groups, whose priority is 1.

## Procedure

1. On a central manager, go to [Manage > Central Management > Enterprise Load Balancer > Associate S-TAPs and Managed Units](#).
2. If you need to create an S-TAP group:
  - a. Click  to open the Create New S-TAP Group dialog.
  - b. Type a name in the Group Name field.  
For example, North\_American\_S-TAPS.  
Recommendation: To ensure compatibility with other Guardium components, do not use spaces or special characters in group names.
  - c. Add group members by selecting from existing host names, or add new members using the Group Member field. S-TAPs indicated with a  are included with the new S-TAP group.
  - d. Click Create New Group to create the S-TAP group.
3. Associate the S-TAP group with a managed units group.
  - a. Select the S-TAP group that you want to associate.  
For example, North\_American\_S-TAPS.
  - b. Click Associate Managed Units to open the Associate Managed Unit Group dialog.
  - c. If necessary, create a new group of managed units.
    - i. Go to [Manage > Central Management > Managed Unit Groups](#).

- ii. Click  to open the Create New Managed Unit Group dialog.
  - iii. Type a name in the Group Name field. For example, `North_American_MUs`.  
Recommendation: To ensure compatibility with other Guardium components, do not use spaces or special characters in group names.
  - iv. Add group members by selecting from existing Managed Unit IP addresses.
  - v. Click Create New Group to create the new group of managed units. The Managed Unit Groups page refreshes, showing the new group.
  - d. Select one or more managed units groups to associate with the S-TAP group.  
For example, `North_American_MUs`.
  - e. Click Apply.
  - f. Click Save to complete the association between an S-TAP group and a managed units group.
4. Optional: Associate the S-TAP group with a managed unit group for failover.
- a. Select the S-TAP group. For example, `North_American_S-TAPs`.
  - b. Click Associate Failover Groups to open the Associate Failover Group dialog. All groups appear in both the associated group and failover group lists. After a group is designated as either an associated group or a failover group, it no longer appears in the other group list.
  - c. If necessary, create a new group of managed units (described in step 3.c).
  - d. Select one or more target managed unit failover groups. For example, `North_American_MUs_failover`.
  - e. Modify the failover priorities of the groups, as relevant.
    - The priority list must be sequential starting with 1.
    - Multiple groups can have the same priority.
    - The priorities cannot skip a level. For example, 1,1,2,3 is valid. However, 1,2,4,5 is invalid.
  - f. Click Apply.
  - g. Click Save to complete the association between an S-TAP group and a failover managed units group.

## Restarting (resynchronizing) S-TAPs for enterprise load balancing

S-TAPs can become unsynchronized for a few reasons, for example, after you modify the S-TAP groups or the managed user groups in your centrally managed environment.

### About this task

S-TAPs can become unsynchronized due to modifications in the Associate S-TAPs and Managed Units page, changes to the S-TAP groups or managed unit groups in other UI pages, scheduler events, and GRD API commands. You can view all unsynchronized S-TAPs in one dialog, and select S-TAPs for restart, which resynchronizes them.

### Procedure

1. Go to `Manage > Central Management > Enterprise Load Balance > Associate S-TAPs and Managed Units`
2. Click Find non-sync S-TAPs.  
The Restart STAPs dialog opens, with a list of all S-TAPs that are not synchronized.
3. Select the S-TAPs that you want to resynchronize and click Restart S-TAPs.

## Viewing the enterprise load balancing load map

Learn how to view the current enterprise load balancer load map.

### About this task

The enterprise load balancing application uses the load information from managed units to create a load map. This load map provides the data that directs load balancing and managed unit allocation activities.

### Procedure

1. To view the current load map as a report in the Guardium® UI, navigate to `Manage > Reports > Unit Utilization > Load Balancer`.
2. It is also possible to view the current load map using the Guardium API. Issue the following GuardAPI command: `grdapic get_load_balancer_load_map`.  
The load map should look like the following example:

```
ID=0

LOAD MAP *****

LOADED MU LIST *****

VACANT MU LIST *****
{
 MU=myguard_01.domain.com
 MU_QUEUE_SIZE(MB)=25.0
 MU_TIMES_REBALANCED=0
 MU_EFFECTIVE_MAX_USED_QUEUE(%)=0.0
 MU_MAX_LOAD_CONTRIB_BY_STAP(MB)=0.0
 MU_ADJUSTED_STAP CONTRIB_IN_MB=0.0
 MU_BASE_MAX_USED_QUEUE_IN_MB=0.0
 IS_REBALANCABLE=true
 INSTALLED_POLICIES=log full details!
 APPLIANCE_RESOURCE_INFO={NUM_PROCESSORS=4,CPU_SPEED=2800,CPU_CACHE=25600,CPU_CORES=4,
 CACHE_READ_RATE=7870,HARD_DRIVE_READ_RATE=186,MEMORY_SIZE=24607}
 STAP_LIST=
}
```

```

 STAP_IP=01_gct1.domain.com, STAP_HOST=01_gct1.domain.com, CONNECTED_TO_MU=gct1.domain.com,
 PARTICIPATES_IN_LOAD_BALANCING=false, MAX_STAP_CONTRIBUTION_TO_LOAD_IN_MB=0.0,
 AVG_STAP_CONTRIBUTION_TO_LOAD_IN_MB=0.0
 }
}
{
STAP_IP=02_gct1.domain.com, STAP_HOST=02_gct1.domain.com, CONNECTED_TO_MU=gct1.domain.com,
PARTICIPATES_IN_LOAD_BALANCING=false, MAX_STAP_CONTRIBUTION_TO_LOAD_IN_MB=0.0,
AVG_STAP_CONTRIBUTION_TO_LOAD_IN_MB=0.0
}
{
STAP_IP=03_gct1.domain.com, STAP_HOST=03_gct1.domain.com, CONNECTED_TO_MU=gct1.domain.com,
PARTICIPATES_IN_LOAD_BALANCING=false, MAX_STAP_CONTRIBUTION_TO_LOAD_IN_MB=0.0,
AVG_STAP_CONTRIBUTION_TO_LOAD_IN_MB=0.0
}
}

***** STAP -> MUS ALLOCATION TABLE *****
03_gct1.domain.com ----> gct1.domain.com
02_gct1.domain.com ----> gct1.domain.com
01_gct1.domain.com ----> gct1.domain.com
ok

```

## Viewing an enterprise load balancing activity report

View a report of enterprise load balancing events and activities.

### About this task

The Enterprise Load Balancer Events report shows all load balancing events and activities, including successful associations between S-TAP agents and managed units, changes in managed unit load, and failed associations. This report can be copied and modified.

### Procedure

To view the report, navigate to **Manage** > **Reports** > **Activity Monitoring** > **Enterprise Load Balancer Events**.

## Enterprise load balancing configuration parameters

Use the load balancer configuration parameters to manage enterprise load balancing. To access the load balancing properties in a central manager, go to **Manage** > **Central Management** > **Enterprise Load Balance** > **Enterprise Load Balance Properties**. In a managed unit, go to **Setup** > **Central Management** > **Registration and Load Balance**.

| Parameter                                        | Default value                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ALLOW_POLICY_MISMATCH_BETWEEN_APPLIANCES         | 1                                                        | Whether the load balancer relocates S-TAP to a managed unit that has a different policy. Valid values: <ul style="list-style-type: none"> <li>0: No</li> <li>1: Yes</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                     |
| APPLIANCE_HW_PROFILE_INDICATORS                  | NUM_PROCESSORS:CPU_SPEED:CPU_CACHE:CPU_CORES:MEMORY_SIZE | The load balancer can account for managed units' hardware profile indicators. The load balancer uses the following column names (as a colon-separated list) from the <i>APPLIANCE_RESOURCE_INFO</i> table to evaluate the hardware profile. Valid values: Column names from the <i>APPLIANCE_RESOURCE_INFO</i> table<br>Under normal circumstances, do not change this parameter.                                                                                                                                                                                                                  |
| DEFAULT_STAP_MAX CONTRIBUTION_TO_MAX_QUEUE_USAGE | 0.1                                                      | When an S-TAP is initially assigned to a managed unit, the load balancer does not have load information about it. The value of this parameter defines the temporary max S-TAP load contribution to the temporary max used queue until the real load is collected from the managed unit (after the interval defined by the <i>TIME_TO_IGNORE_STAP_CONNECTION RELATED LOAD</i> parameter).<br>Valid values: 0.1 to 1 in increments of 0.1<br>Under normal circumstances, do not change this parameter.                                                                                               |
| DEFAULT_STAP_MAX_QUEUE_USAGE                     | 0.15                                                     | When an S-TAP is initially assigned to a managed unit, the load balancer does not have load information about it. The value of this parameter defines the temporary sniffer max used queue until the real load is collected from the managed unit (after the interval defined by the <i>TIME_TO_IGNORE_STAP_CONNECTION RELATED LOAD</i> parameter).<br>Valid values: 0.10 to 1 in increments of 0.10<br>Under normal circumstances, do not change this parameter.                                                                                                                                  |
| DISK_USAGE_ADJUSTMENT_FACTOR                     | 100                                                      | The percentage of the managed unit's system var disk usage that is compared to the unit utilization threshold 1. If the disk usage * DISK_USAGE_ADJUSTMENT_FACTOR is greater than Threshold 1, then the managed unit is considered loaded.<br>For example, DISK_USAGE_ADJUSTMENT_FACTOR = 50, and the 'utilization thresholds' system var disk usage threshold 1 = 40. The managed unit is considered loaded if the system var disk usage is 80 or higher, since 50% * 80 meets the threshold of 40. For more details, see <a href="#">Unit utilization and Unit utilization details reports</a> . |
| ENABLE_DYNAMIC_LOAD_COLLECTION                   | 1                                                        | Controls the load collection method. Valid values: <ul style="list-style-type: none"> <li>0: Disables the dynamic load collection interval (uses <i>STATIC_LOAD_COLLECTION_INTERVAL</i> as the collection interval).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                    |

|                                                         |       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                         |       | <ul style="list-style-type: none"> <li>• 1: Enables the dynamic load collection interval. The collection interval is proportional to the number of managed units (1 hour per 10 connected managed units).</li> </ul> <p>Changing this parameter triggers an immediate recalculation of the next full load collection time.</p>                                                                                                                                                                                                                                                                                          |
| ENABLE_FAILOVER_GROUPS_REBALANCE                        | 1     | <p>Controls automatic relocation of S-TAP from the failover group back to the main managed unit group when a managed unit in the main managed unit group is available again. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Disable.</li> <li>• 1: Enable.</li> </ul>                                                                                                                                                                                                                                                                                                                                    |
| ENABLE_RELOCATION                                       | 1     | <p>Relocation of resources (rebalancing) is a process that the load balancer runs after full load collection. Relocation here means transferring S-TAPs from loaded managed units to less loaded managed units. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Disable.</li> <li>• 1: Enable.</li> </ul>                                                                                                                                                                                                                                                                                                 |
| EVALUATE_ADDITIONAL_LOAD_INDICATORS                     | 0     | <p>Evaluate additional load indicators when you classify a managed unit as loaded. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Disable.</li> <li>• 1: Enable.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                              |
| LOAD_BALANCER_ENABLED                                   | 1     | <p>Controls the load balancer feature. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Disables the load balancer.</li> <li>• 1: Enables the load balancer.</li> </ul> <p>If disabled on the managed unit, the load balancer (running on the central manager) does not collect load information from that managed unit. All the S-TAPs connected to that managed unit do not participate in load balancing.</p> <p>On the central manager, enabling this parameter (after it was disabled) triggers an immediate full load collection from all the managed units that are enabled for load balancing.</p> |
| 12.1 and later<br>LOAD_SAMPLING_METHOD                  | AVG   | <p>Controls the sniffer load during the sampling period. Valid values:</p> <ul style="list-style-type: none"> <li>• AVG: Controls the average sniffer load.</li> <li>• MAX: Controls the maximum sniffer load.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                               |
| LOADED_SNIFFER_QUEUE_USAGE_THRESHOLD                    | 0.6   | <p>A managed unit is considered loaded if its sniffer has at least one queue whose size reaches the LOADED_SNIFFER_QUEUE_USAGE_THRESHOLD.</p> <p>Valid values: 0.10 to 1 in increments of 0.10</p> <p>Under normal circumstances, do not change this parameter.</p>                                                                                                                                                                                                                                                                                                                                                     |
| MAX_CONCURRENT_LOAD_COLLECTIONS                         | 10    | <p>The maximum number of concurrent load collection processes the load balancer runs at any point in time. That is, the number of concurrent, nonpersistent, remote SQL connections from the central manager to the managed unit.</p> <p>Valid values: ≥1</p>                                                                                                                                                                                                                                                                                                                                                           |
| MAX_RELOCATIONS_BETWEEN_FULL_LOAD_COLLECTIONS           | 3     | <p>Defines the maximum number of S-TAP relocations (between managed units) allowed after a full load collection.</p> <p>Valid values: ≥-1</p> <p>Negative values indicate that unlimited relocations are allowed.</p>                                                                                                                                                                                                                                                                                                                                                                                                   |
| MAX_RELOCATIONS_PER_MU_BETWEEN_FULL_LOAD_COLLECTIONS    | 3     | <p>The maximum number of S-TAP relocations allowed from a specific managed unit during any one period of full load.</p> <p>This parameter is the maximum number of STAPs that can be relocated per managed unit. If you have two loading S-TAPs, and the value is set to 1, then only one of these S-TAPs can be moved for a specific managed unit. If the value is set to 0, then STAP does not relocate.</p> <p>Valid values: ≥-1</p> <p>Negative values indicate that unlimited relocations are allowed.</p>                                                                                                         |
| REBALANCE_IF_MU_CLASSIFIED_AS_LOADED_N_TIMES_IN_M_HOURS | 1:168 | <p>Loaded managed units can be rebalanced only if they are classified as loaded for a specified number of instances over a specified period of hours. For example, a value of 1:168 requires that a managed unit is classified as loaded at least 1 time during a period of 168 hours.</p> <p>Valid values: ≥0 : ≥0</p>                                                                                                                                                                                                                                                                                                 |
| STATIC_LOAD_COLLECTION_INTERVAL                         | 720   | <p>Static managed unit load collection interval (in minutes).</p> <p>If ENABLE_DYNAMIC_LOAD_COLLECTION is set to 0, the load balancer collects the load from all the managed units at the interval that is specified by STATIC_LOAD_COLLECTION_INTERVAL.</p> <p>Valid values: ≥10</p>                                                                                                                                                                                                                                                                                                                                   |
| TIME_TO_IGNORE_STAP_CONNECTION RELATED_LOAD             | 10    | <p>When you collect the load statistics for S-TAPs of each managed unit, avoid including data that represents the initial S-TAP connection to the managed unit. This data can indicate traffic spikes that create a false-positive for the load balancer. This parameter tells the load balancer to ignore S-TAP load for the specified number of minutes after the S-TAP is connected to the managed unit.</p> <p>Valid values: ≥5</p>                                                                                                                                                                                 |
| USE_APPLIANCE_HW_PROFILE_FACTOR                         | 1     | <p>The load balancer can use managed units' hardware profile indicators (specified by the parameter APPLIANCE_HW_PROFILE_INDICATORS) when it evaluates vacant managed units for relocating S-TAPs. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Ignores hardware profile indicators.</li> <li>• 1: Uses managed unit hardware profile indicators.</li> </ul>                                                                                                                                                                                                                                           |
| USE_IP_ADDRESS_F                                        | 0     | Whether the load balancer returns the addresses of S-TAP allocated managed units as a list of hostnames or IP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

|                        |                                                                                                                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FORMAT_FOR_ALLOCATIONS | addresses. Valid values: <ul style="list-style-type: none"><li>• 0: Returns a list of hostnames for S-TAP allocated managed units.</li><li>• 1: Returns a list of IP addresses for S-TAP allocated managed units.</li></ul> |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Related reference

- [Central management APIs](#)

## Deployment inventory

The inventory view provides centralized view of all database servers and any installed S-TAPs or GIM clients.

Note: S-TAP points to a single primary collector and possibly multiple secondary collectors for load balancing. If you change the primary collector from the Central Manager, it reflects in the Deployment inventory table within 5 minutes. The table displays primary collector label in the Collector column to indicate the primary collector.

## Resource deployment view

The resource deployment view shows the GIM clients and S-TAPs installed on the database servers in a Guardium environment.

## Monitoring managed units

Monitor managed units from the Guardium Central Management page.

To monitor and manage managed units,

1. Log in as an admin user to the Guardium® GUI of the central manager for the units you want to view or manage.
2. Click [Manage > Central Management > Central Management](#) to open Central Management page.

The Central Management page is divided into two sections, the Central Management table, and the Selected Units section. From the Selected Units section, you can select several management tasks that you can perform on selected units. The information and tasks are described in the following tables.

Click any column in the Central Management table to sort the table in ascending order. Click again to sort in descending order.

Table 1. Central Management table. View information about all the managed units for this central manager and select and manage the managed units.

| Control or header         |                                                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Groups                    |                                                                                     | <p>Lists the names of all available groups. You can either select All Units group to see all the units associated with this central manager, or select another group to see a subset of managed units.</p> <p>The All Collectors and All Aggregators groups are always available (along with the All Units group). In addition, any groups that you create, or that are automatically created for you, also display in the Groups list.</p> <p>You can create and manage groups by clicking Group Setup  in the Selected Units section of the Central Management window. For more information, see <a href="#">Group Setup</a> or <a href="#">Creating managed unit groups</a>.</p> |
| Select all checkbox       | <input type="checkbox"/>                                                            | Select the checkbox in the heading to select all managed units (and clear the checkbox to deselect all managed units).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Checkbox                  | <input type="checkbox"/>                                                            | Select a specific unit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Refresh unit information. |  | Refreshes all information that is displayed in the expanded view of that unit and issues new requests to that unit. This action also causes a full user synchronization cycle.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Reboot unit               |  | Reboots the unit at the operating system level. By default, the Guardium portal is started at startup.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Restart unit portal       |  | Restarts the Guardium application portal on the selected managed unit. You can then log in to that unit to perform Guardium tasks (defining or removing inspection engines, for example).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Shortcut to unit portal   |  | Opens the Guardium login page for the managed unit, in a separate browser window.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Unit                      |                                                                                     | <p>The hostname of the managed unit.</p> <p>If the hostname changes on the unit, the central manager no longer sees that unit when the online status is automatically refreshed. If you suspect the hostname was changed, click Refresh on the toolbar. Guardium updates the hostname and online status as needed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Online                    |  | <p>Indicates whether the unit is online.</p> <ul style="list-style-type: none"> <li>• Green light - Unit is online.</li> <li>• Red light - Unit is offline.</li> </ul> <p>Hover the mouse pointer over the stoplight icon to display the IP address as a tooltip.</p> <p>All the units are checked (pinged) periodically by a background process. The status is refreshed whenever the machine is checked. See the Last Ping column for the most recent refresh time.</p>                                                                                                                                                                                                                                                                                              |
| Installed Policy          |                                                                                     | A link to the security policy that is installed on the managed unit. This field is updated on every ping.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Control or header     |  | Description                                                                                                  |
|-----------------------|--|--------------------------------------------------------------------------------------------------------------|
| Installed Policy Date |  | The date and time the policy was installed.                                                                  |
| Unit Type             |  | The type of unit (such as Managed Aggregator or Managed Collector) and the IP mode.                          |
| Ver.                  |  | The Guardium version number of the managed unit.                                                             |
| Last Patch            |  | The most recently installed patch number.                                                                    |
| Last Ping             |  | The last time that the unit was pinged by the central manager to determine the managed unit's online status. |

Table 2. Selected units section

| Button                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group Setup                                    | Opens the Group Setup window, from which you can create new groups, remove groups, and associate managed units with groups. For more information, see <a href="#">Creating managed unit groups</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Unregister                                     | Unregister all selected units.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Reboot                                         | Reboot the selected managed units.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Restart Portal                                 | Restart the Guardium portal for the selected units.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Restart Inspection Engines                     | Restart the inspection engines of the selected units.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Refresh                                        | Refresh the names and other information for the selected units.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Install Policy                                 | Opens the Install Security Policy page. Select a policy to apply to all selected units. For more information, see <a href="#">Installing security policies on managed units</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Patch Distribution                             | Patch Distribution opens the Patch Distribution page, which displays a list of available patches with dependencies. You can select a patch and install it on all selected units. You can also schedule patches up to one year in the future. For more information, see <a href="#">Central patch management</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Distribute Uploaded Jar Files                  | <p>Click Harden &gt; Vulnerability Assessment &gt; Customer Uploads. Then, enter the name of the file to be uploaded. Otherwise, click the Browse to locate and select that file. Upload one driver at a time.</p> <p>Click Upload. You are notified when the operation completes, and the file that is uploaded is displayed. This action brings the uploaded file to the central manager.</p> <p>Select the managed unit or units where you want to distribute the JAR files. Click Distribute Uploaded JAR files.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Distribute Patch Backup Settings               | This setting distributes the following to selected units:<br><br>PATCH_BACKUP_FLAG; PATCH_AUTOMATIC_RECOVERY_FLAG; PATCH_BACKUP_DEST_HOST; PATCH_BACKUP_DEST_DIR;<br>PATCH_BACKUP_DEST_USER; PATCH_BACKUP_DEST_PASS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Distribute Authentication Config               | Distribute the authentication configuration to all managed units selected. For more information, see <a href="#">Distributing authentication configuration</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Distribute Configurations                      | <p>The following configurations are distributed to sync parameters between the central manager and the managed units:</p> <ul style="list-style-type: none"> <li>• Anomaly Detection - Active on startup, Polling interval</li> <li>• Alerter - all fields</li> <li>• Data Archive - all fields</li> <li>• Global profile - Concurrent Logins, Data Level Security, all fields except Named Templates (which are already synced), PDF footer text, and logo image.</li> <li>• IP-to-Hostname Aliasing - both check boxes</li> <li>• Results Archive - all fields</li> <li>• Results export - all fields</li> <li>• Session Inference - all fields</li> <li>• System Backup - all fields</li> <li>• Data export - all fields</li> </ul> <p>Some of these configurations do not take effect until the portal is restarted (Anomaly Detection, Session Inference). Other processes, such as the Alerter, need to be restarted, either directly through the admin portal of the managed unit, or by rebooting all relevant managed units from the manager. For more information, see <a href="#">Distributing configurations</a>.</p> <p>Distribute Configurations does not restart the managed units. To restart the managed units, either select the restart unit icon ( for a single unit or select Restart Portal to restart all the selected units.</p> <p>For any configuration that includes scheduling , you can select the Include Schedule checkbox. When Include Schedule is selected, Distribute Configurations also includes the configuration's scheduling.</p> |
| Distribute GIM bundles                         | Distributes GIM bundles to the selected managed units. A message displays when the GIM bundles are distributed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Register New                                   | Opens the Unit Registration page to register a new unit for management.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Patch Installation Status                      | Opens the Patch Installation Status window, which displays failed installations and discrepancies for each unit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Designate Backup CM                            | Displays the Designate Backup CM window. Select a backup central manager IP address or select a unit that can serve as the backup central manager and click Apply.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 12.1 and later Run database instance discovery | <p>Runs the database instance discovery from the central manager on all the active Unix or Windows S-TAP units for all the managed units, a group of managed units, or a single managed unit.</p> <p>Opens the Run database instance discovery page, where you can select all managed units, a group of managed units or an individual managed unit, all active S-TAP hosts, and the Replace Inspection Engines checkbox.</p> <p>Important: Do not check <b>Replace Inspection Engines</b> unless you want to overwrite the existing inspection engine configurations. You can view the discovered instances under Discover &gt; Reports &gt; Discovered Instances.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

# Assigning correlation alerts from the central manager to individual managed units or managed unit groups

You can assign correlation alerts to individual managed units or managed unit groups from the central manager. You can assign or exclude alerts to a unit or to a managed unit group. You can also specify whether to run the alerts on the central manager itself. For more information, see [Managing correlation alerts](#).

Notes:

- On the individual managed units, the alert builder does not show any section on managed units. Only the central manager can assign alerts to units and groups.
- For any entries in the alert table that exclude a given managed unit, a system-generated group is created to exclude that unit for each excluded alert. The group is created when the alerts are started on that managed unit.
- The alert windows on the anomaly detection page under admin console were used to locally enable or disable alerts. For this feature, the alert windows appear only on the central manager.
- On the managed units, a table shows active alerts and whether they are enabled.

## Creating managed unit groups

Organize managed units into groups and then take actions on those groups.

### About this task

Managed unit groups allow you to organize managed units into meaningful groups and then take actions on those groups. For example, you might create managed unit groups for specific unit types, geographies, or lines of business. Actions you might take include installing policies or distributing patches or configurations to a group of managed units.

Guardium® has two predefined groups that account for all managed units: All Aggregators, and All Collectors. When you add a managed unit to your system, it is automatically added to one of these groups. These two groups are mutually exclusive.

When you restore a unit from the backup taken from the different environment that contains appliances that are not registered to the new restored system, go to the Managed Unit Groups page in the new environment and modify the groups accordingly. If there are distributed reports based on these groups, they are corrected automatically when you save the changes in the Managed Unit groups page.

### Procedure

1. Go to [Manage > Central Management > Managed Unit Groups](#).
2. Click to create a new managed unit group or to edit an existing group.
3. In the Create new managed unit group dialog, type a name for the group in the Group name field.  
Recommendation: To ensure compatibility with other Guardium components, do not use spaces or special characters in group names.
4. Use the icons to select managed units to include in the group.
5. When you have finished selecting managed units to include in the group, click Save.  
The new managed unit group is saved and appears on the Managed Unit Groups page.
6. Optionally, from the Managed Unit Groups page, click the icon to expand a group and view its managed units.

### Results

Once defined, a managed unit group is available from the [Manage > Central Management > Central Management](#) page, the [Manage > Central Management > Distribute Configuration Profiles](#) page, as a managed unit group within the [Manage > Central Management > Enterprise Load Balance > Associate S-TAPs and Managed Units](#) tool, and in other locations where managed unit groups are used.

## Installing security policies on managed units

Install a security policy on a manage unit.

### About this task

To install a security policy on a managed unit:

### Procedure

1. Click [Setup > Tools and Views > Policy Installation](#) to open Currently Installed Policies and the Policy Installer.
2. From the Policy list, select the policy that you want to install.
3. From the list, select an installation action. After you select an installation action, you are informed of the success (or failure) of each policy installation. If a selected unit is not available (it might be offline or a link might be down), the Central Manager informs you of that fact. It continues attempting to install the new policy for a maximum of seven days (on the condition that unit remains registered for central management).
4. From the Policy list, select the policy that you want to install.
5. The available installation actions include the following items:
  - a. Install and Override - delete all installed policies and install the selected one instead
  - b. Install last - installing the selected policy as the last one in the sequence; installing the policy after all currently installed policies and having the lowest priority
  - c. Install first - installing the selected policy as the first one in the sequence; installing the policy before all currently installed policies.

Note: If you install a policy from the Central Manager, the selection of Run Once Now (and scheduler) updates existing groups within the installed policies.

To load changes to rules, including addition and subtraction of groups, you must either:

- a. Initially install policies from the Collector, or
- b. Reinstall policies from the Collector or Central Manager.

## Central patch management

Provide visibility and control over patch installation, status, and history.

### About this task

The central manager provides the interface to install patches on all managed units in your environment and also view the patch installation status and history for each unit. After your central manager is upgraded, you can use its interface to also view the detailed patch status log for each managed unit even if the units are running on an older version.

When you install a patch, a date and time request can be specified to indicate when the patch is installed. If no date and time is entered or if now is entered, the installation request time is immediate.

Note: A patch that is installed successfully can be installed again. This fact is important for batched patches. A warning informs you if the patch is already installed. Log in to the Guardium® GUI of the unit to be managed as the admin user:

### Procedure

1. Click **Manage > Central Management > Central Management**.
2. Select the units that need the patch, and click **Patch Distribution**.
3. From the Patch Distribution screen select the patch you want to distribute and click **Install Patch Now** or **Schedule Patch**.
4. To see the summary of the installation status, click **Manage > Central Management > Central Management** and then select the units and click **Patch Installation Status**. The summary lists all the patches for each managed unit in the order that the installation was requested. The Patch Installation Status screen also displays, for each unit, failed installations and discrepancies. For example, having one patch installed on part of the units only, regardless if it failed on other units or was not installed. To remove patches from the Patch Distribution screen, click the delete icon (red x) next to the patch. This does not delete the patch from the patch distribution directory on the appliance, but will remove it from the display.  
Attention: Removing a patch from the patch distribution display also removes that patch from dependency-checking and can prevent the installation of newer patches.
5. To see detailed information about the patch installation, click on a managed unit that is listed under the Unit name column. This action opens the **Patch Status Details** window, where you can view the last five lines of the patch status log for the managed unit. The patch status log reflects the last patch that was installed. If a patch installation is in progress, the latest patch log is displayed. If you'd like to see more details from the log, click **Fetch More**.
6. When you click on a different managed unit, the log in the **Patch Status Details** window is appended. You also have the ability to **Clear** or **Close** the log, as needed.  
Important: To view the patch status details, the root passkey must be installed on the managed unit. If the root passkey is not installed, you will receive an error message. For more information, see [Resetting the root password](#).

## Distributing authentication configuration

Instead of configuring authentication on each appliance separately, central management authentication (Configure Authentication) can be configured once on the central manager and then distributed to all managed units. This way, information is entered once and it applies to some or all units; some of the units may have a different type of authentication.

### Procedure

1. Ensure authentication (Configure Authentication) on both the central manager and the managed unit. So if LDAP authentication is being used, ensure that LDAP is configured on the central manager and the managed unit.
2. Select the managed units to receive the distribution of the central management authentication.
3. Click **Distribute Authentication Config** to distribute the authentication configuration to all managed units selected.

## Distributing configurations

Configurations and their schedules, can be distributed, either all or individually, between the central manager and the managed units.

### Procedure

1. Select the managed units that receive the configurations.
2. Click **Distribute Configurations** to display the **Distribute Configurations** window.
3. Check the appropriate boxes for the configurations that you want to distribute. Use the check box in the header to select all configurations.
4. Check the appropriate boxes for any schedules that you want to distribute. Use the check box in the header to select all schedules. If a configuration is not scheduled, the check box is not available.
5. Click **Distribute** to distribute the configurations and schedules.

## What to do next

After you distribute the configuration, you might need to either reboot or restart any managed units that you have updated.

#### Alerter

Restart managed units.

If Active on Startup is selected, the alerter starts each time the appliance restarts.

GUI restart does not take the Active on Startup value.

The alerter must be manually restarted on the managed units through the admin portal (Admin Console > Alerter). Since you cannot restart the alerter from the central manager, restart the managed units from the Admin Console for the same effect.

#### Anomaly Detection

Restart managed units.

If Active on Startup is selected, anomaly detection starts each time the appliance restarts.

GUI restart takes the Active on Startup value.

#### Session Inference

Restart managed units

If Active on Startup is selected, session inference starts each time the appliance restarts.

GUI restart takes the Active on Startup value.

#### Results Export, System Backup, Data Archive, Result Archive, and Data export

No restart or reboot needed. The configuration is distributed automatically.

#### Global profile

No restart needed. However, using a different named template applies only when policy is installed.

Note: When you distribute the configuration for the global profile, the following values are distributed:

- ACTIVATE\_ALIASES
- CUSTOM\_DB\_MAX\_SIZE
- CHECK\_CONCURRENT\_LOGIN
- HTML\_BOTTOM\_RIGHT
- HTML\_BOTTOM\_LEFT
- DISPLAY\_LOGIN\_MESSAGE
- LOGIN\_MESSAGE
- CSV\_DELIMETER
- FILTERING\_ENABLED
- INCLUDE\_CHILDREN\_ON\_FILTER
- SHOW\_ALL\_RECORDS
- ACCORDION\_DISABLED
- SCHEDULER\_RESTART\_INTERVAL
- SCHEDULER\_RESTART\_WAIT\_SHUTDOWN
- ESCALATE\_TO\_ALL
- MESSAGE\_TEMPLATE

---

## Working with configuration profiles

Configuration profiles allow you to define configuration and scheduling settings from a central manager and distribute those settings to managed unit groups without altering the configuration of the central manager itself.

### Before you begin

Before creating and distributing configuration profiles, verify the following prerequisites:

- Allow communication over port 8447 between the central manager and its managed units
- The central manager and the managed units that will receive configurations must be at or above Guardium® V10.1

### About this task

Configuration profiles contain two types of information: configuration type (one or more sets of configuration and scheduling settings), and a list of managed unit groups to be updated with the configuration and scheduling settings. Once defined, configuration profiles can be stored, modified, and reused to distribute specific sets of configuration and scheduling settings to specific groups of managed units.

The configuration types you can add to a configuration profile are:

- Alerter
- Audit process schedules
- CyberArk upgrade configuration
- Data archive
- Data export
- Data import schedule
- Data streaming configuration
- Database discover instances rules schedule
- Flat log process
- Ip-to-hostname aliasing
- Kerberos
- PIM data correlation
- Policy installation schedule
- Results archive (Audit)
- Results export (Files)
- Session Inference
- System backup
- Unit utilization schedule
- Unit utilization thresholds

Configuration profiles are defined independently of the local settings on the central manager. This allows you to quickly define configuration settings and deploy those settings to managed unit groups without disrupting the configuration of your central manager or configuring each managed unit individually.

This task describes how to create, distribute, and save a configuration profile.

## Procedure

---

1. Navigate to [Manage > Central Management > Distribute Configuration Profiles](#).
2. Click or select an existing profile to begin working with a configuration profile.
3. From the Name and description panel, provide a name and optionally provide a description for the profile. Click Next to continue.
4. Optionally, click Roles to specify security roles that can use the configuration profile.
5. From the What to distribute panel, click to define a new configuration, or select an existing configuration and click to edit.
  - a. From the Configuration type menu, select a configuration type to add to the profile.
  - b. Specify configuration and scheduling details for the selected configuration type.  
Restriction: Distributing data export configuration settings to an aggregator do not distribute any purge settings. The existing purge settings on an aggregator are retained. On collectors, purge settings, including retention periods, are distributed to and replace existing purge settings.
  - c. Click Save to finish editing the configuration profile.
  - d. Optionally, add additional Configuration Types/schedules by clicking , and repeating steps [5.a](#) through [5.c](#).
  - e. Click Next to continue.
6. From the Where to distribute panel, select groups from the Managed unit groups table and use the icon to add the groups to the Selected groups table. Click Next to continue.  
Note: Click to create a new managed unit group or to edit an existing group. Managed unit groups can also be defined and edited at [Manage > Central Management > Managed Unit Groups](#).
7. Optionally, from the Distribute configurations panel, click Run Now to distribute the configuration profile to the selected groups. When the status indicates that distribution is complete, click Next to continue.
8. From the Review results panel, review a summary of the distribution process and its results.  
Optional: click Run Log to view a detailed log of the distribution process.
9. Click Save to save the configuration profile for reuse.

## What to do next

---

If you need to move configuration profiles between central managers, use [Manage > Data Management > Definitions Export](#) and [Manage > Data Management > Definitions Import](#) and select Configuration profile from the Type menu.

## Related concepts

---

- [Configuring the alerter](#)
- [Data aggregation](#)
- [Database discovered instance rules scheduler](#)
- [Exporting and importing definitions](#)
- [IP to Hostname Aliasing](#)
- [Scheduling](#)

## Distribute custom tables

---

Distribute custom tables and their data from a central manager to managed units.

## Before you begin

---

Distributing custom tables from a central manager to managed units requires that the table structure on the managed units match the table structure on the central manager. Distribution fails if the tables are altered only on the managed units.

## Procedure

---

1. Navigate to [Comply > Custom Reporting > Custom Table Distribution](#).
2. Use the check boxes to select tables for distribution.  
The list includes all custom tables available on the central manager. The tables you select are distributed to all managed units that report to the central manager.
3. In the Scheduling section, define a recurring schedule for distributing custom tables.
4. Click Save.
5. Optional: Click Run Once Now to submit an ad hoc job for custom table distribution.

## Results

---

The selected tables and their data are distributed from the central manager to its managed units according to the defined schedule.

Attention: When distributing tables, if a table with the same name exists on a managed unit, the table and all of its data are replaced on the managed unit.

## Central manager redundancy

---

Use Central Manager Redundancy or Backup Central Manager (CM) to configure a secondary or backup CM in case the Primary CM becomes unavailable.

Central Manager redundancy supports the following:

- Backup Central Manager - Make Primary CM link is available after the primary central manager loses connection.
- User Layouts are retained.
- User and roles are in the sync backup and do not rely on Portal User Sync.
- User Group Roles Data are retained.
- An API function `make_primary_cm` allows you to switch the central manager from the CLI.
- Data is retained from Audit Process Builder processes after switching Primary Central Manager to Backup Central Manager.
- Central Management backup includes all the definitions (reports, queries, alerts, policies, audit processes etc.), users and roles as it did before.
- It includes the schedules for enterprise reports, distributed reports and LDAP.
- It includes schedules for all audit processes; schedules and settings for data management processes such as archive, export, backup, and import; populate group members from query.
- It includes settings for Alerter and Sender.
- User's GUI customization's, custom classes and uploaded JDBC drivers are included.

Note:

- Data, either collected data, audit results and custom tables data, is not included.
- The Top risky users list and threat cases are not copied to the backup central manager.
- To list status of `cm_sync_file`(s) on Backup CM, use the CLI command, `show local_cm_sync_file`. To list the value of Backup CM IP for each managed unit, use the GuardAPI command, `grdapic show_backup_cm_ip` (this API command can only run on a central manager).
- Failover with Central Manager load balancing - After failover, if the new managed units connect and then disconnect right away, the correct DB\_USER is not sent until the failover message is received.
- Switching to a backup central manager interrupts communication with collectors and may generate the following message: "Central manager experienced failed data transfer from collector." The issue is visible in the Scheduled Jobs Exceptions report and should clear within 24-hours.

Perform these steps on your development or secondary servers and test. If successful, then perform these steps on your Primary or live Guardium Servers.

Install Patches on Central Manager

1. From the now Primary CM, login as CLI.
2. Install patches with the following CLI command, `store system patch install scp`
3. This CLI command will copy the files over to your Guardium Server and give you the ability to install them.
4. Watch these patches being installed with the following CLI command, `show system patch install`
5. Wait until the patch status shows "DONE: Patch installation Succeeded." for both patches.

Install Patches on Backup CM

1. Login into the now Primary CM GUI as admin.
2. Navigate to `Manage > Central Management > Central Management`.
3. Click check box for the Backup CM managed unit ONLY on the Central Manager.
4. Click Patch Distribution and install all of the patches that you just installed onto the Primary CM.

Example to install a patch:

1. Click Patch Distribution.
2. Click Install Patch Now.
3. Wait approximately 15 minutes to be sure the patch is installed on all managed servers.
4. To verify, login as CLI on the Backup CM and run CLI command, `show system patch install`, from Backup CM server.

Install Patches on all other managed servers (optional steps)

1. Repeat the previous steps to install patches on all managed servers.
2. Verify that all patches have been installed before going to the next procedure.

After all Patches have been installed on the CM and managed servers

1. Login as admin onto the now Primary CM.
2. Navigate to `Manage > Central Management > Central Management` and click Designate Backup CM.
3. Select Backup CM server from the returned list of eligible Backup CM candidates.
4. Click Apply.
5. Wait approximate two minutes for the Backup CM to sync and the NEW Backup CM file to be created and copied to the Backup CM.
6. Wait for two complete rounds of backups to complete (approximate 1 hour) for two Backup CM sync files that will be copied to the Backup CM and can be viewed from the Guardium Monitor tab - Aggregation Archive Log Report.
7. Select Guardium Monitor and select Aggregation/Archive Log Report to view the progress of the creation of the Backup CM sync file.
8. Verify the Activity Backup has started and the `cm_sync_file.tgz` file has been created from the Aggregation/Archive Log Report.
  - a. Login as Admin from the GUI.
  - b. Select Guardium Monitor tab.
  - c. Select Aggregation/Archive Report.
  - d. Look for Backup Types.
9. When complete:
  10. The patches have been installed on the CM.
  11. The patches have been installed on the Backup CM.
  12. Option: The patches have been installed on all other managed units.
  13. Two Backup CM Sync files have been completed (see Aggregation/Archive Log file under Guardium Monitor Tab).
  14. The following steps outline the process to convert the now Primary CM and its managed nodes to the Backup CM.
    - IMPORTANT: Wait approximately one hour to be sure at least TWO of the Backup CM sync files supporting Backup CM have completed.
    - The backups schedule for Backup CM sync files is approximately every 30 minutes.
    - The process will run on the CM to create a backup CM file and copy that file to the directory on the Backup CM.

Start the Backup CM Process after two sync file process have completed

## Shutdown the Primary CM Guardium Server

If you have no access to shutdown the Primary CM, then go directly to the Backup CM and login as Admin. Navigate to [Manage > Central Management > Central Management](#) and click Make Primary CM. Skip to the section "Steps to start the Backup CM configuration to become the Primary CM" in this document.

1. Wait approximate five minutes and login again as admin in the GUI of the Backup CM.
2. Once the Primary CM is shutdown completely, you can continue onto the next step

If you are logged into the Primary CM and it goes down, you get a message indicating that the connection has timed out.

## Steps to start the Backup CM configuration to become the Primary CM

The secondary CM will not be responsive for approximately five minutes. Login after five minutes and the Make Primary CM link will be available. The link is available under the admin login at [Manage > Central Management > Central Management](#).

1. When the Primary Server goes down, you will get a message on the Backup CM "Unable to connect to Remote Manager, consider switching to (the name of the backup CM)".
2. If you decide to switch:
  - a. Login as admin
  - b. Navigate to [Manage > Central Management > Central Management](#).
  - c. Click Make Primary CM (do not click the "Make Primary CM" link more than once. Also stay on this screen and do not select anything else during the running of this process. A log file will be created that you can view to see the progress and completion of this process.) Be patient as this process will take awhile to complete. There is a safeguard that if you do click this button more than once nothing will change with the current running process.
  - d. Within seconds you should get a message "Are you sure you want to make this unit the primary CM? Click OK."
  - e. Within a few seconds more you will get a message stating "This may take a few minutes". The time it takes for the Backup CM to become the primary CM depends on the amount of data backed up from the Backup CM sync file and the amount of managed nodes that switch to the Backup CM which will become the Primary CM. Click OK. As soon as we click OK a log file will be created called `load_secondary_cm_sync_file.log` that will allow you to view the progress of the switch to the completion of the Backup CM switch process. This file can be viewed from your GUI. The following steps indicate how to view this log file.
  - f. The last message will take a while to be presented to the screen. It will be the last message before the Backup CM switch has completed. The message is "GUI will restart now. Try to login again in a few minutes and the Backup CM will now become the Primary CM". Click OK. Wait a few minutes for the Backup CM to become Primary and for all the managed nodes to complete switching over to the new Primary CM.

While the CM Backup Process is running – viewing the progress log file

From the Backup CM while the Make Primary CM process is running, you can do the following to view the progress of the Backup CM becoming the Primary CM.

Prerequisite: You will need the IP of the server you are connected to in order to view the log files.

1. Login as CLI from your Backup CM server from a Putty.exe session
2. From CLI run Fileserver <IP> "enter your IP number" 3600", for example: fileserver 9.70.32.122 3600
3. From the GUI, enter the value: <http://yourserver.x.x.x.com> (will display in the CLI screen after entering the command, example: <http://joe.server.guardium.com> (the server name will be the Backup CM server).  
Fileserver Window on the UI will open to select file – Select Sqlguard logs
4. Select the file: `load_secondary_cm_sync_file.log`. (The file will display in a list of files from Step #3.) This will allow you to view the progress of the Backup CM becoming the Primary CM. Locate log file for viewing  
CM Backup Process is complete when you see this line in the `load_secondary_cm_sync_file.log`  
Import CM sync info - DONE
5. Wait approximately 10 minutes for all the Managed units to become available to the New Primary CM.

After the Backup CM becomes the Primary and all Managed nodes are now managed by the Backup CM server

You can now bring up the old CM server. Once it is up and running, perform the following steps to add it as the Backup CM server.

1. Reboot Old Primary CM.
2. Once the Server is up, login as CLI.
3. Delete the manager unit type, enter delete unit type manager.
4. After it completes and you get an OK message from CLI.
5. VERY IMPORTANT: Wait approximately five minutes for the GUI to completely restart even after the deleted unit type displays a successful message and the GUI restart message.
6. After five minutes, log into the New Primary CM to register Old CM as a managed unit.
7. Login as admin on New Primary CM.
8. Navigate to [Manage > Central Management > Central Management](#).
9. Click Register New.
10. Enter IP of the Old Primary CM that you just rebooted.
11. Enter 8443 as Port.
12. Click Save. (IMPORTANT: Be patient, do not click this button twice).
13. Wait a minute for the Old Primary CM to become registered.
14. Make the Old Primary CM a New Backup CM.
15. Click Designate Backup CM.
16. Click on Old Primary CM server.
17. Click Apply.
18. Old Primary CM server is NOW the New Backup CM server.
19. Refresh Central Management screen to see the New Unit type Backup CM defined.
20. This task is complete.

Report Data After Backup CM Process is complete

The following data is missing after the Backup CM process is completed. This is related to only the "first" switch from the Primary to the Secondary CM.

Missing Data:

1. Audit Process Results
2. Custom Table Data
3. Custom Report Data
4. VA Results
5. Classifier Results

6. DSD Results
7. CAS results
8. Datamart Data
9. Collected Data
10. Entitlement Data

The reports are populated again once you run these reports again on the New Primary CM. If you switch back to the old Primary CM, the data for these reports will be presented.

## Managing your Guardium system

Management tasks include monitoring your system's health and managing artifacts such as groups, domains, and notifications.

- [\*\*Guardium Administration\*\*](#)  
Guardium® administrators perform various administration and maintenance tasks.
- [\*\*Certificates\*\*](#)  
Install certificates so you can connect to the Guardium GUI, and for Guardium-S-TAP communication. Check certificates regularly, so you can update them before they expire.
- [\*\*Alerts\*\*](#)  
Learn how to work with alerts.
- [\*\*System performance and monitoring\*\*](#)  
Learn to use Guardium tools to maintain system performance: unit utilization reports to identify under- and over-utilized systems; system self-monitoring; and the Services status page.
- [\*\*Scheduling\*\*](#)  
The general-purpose scheduler is used to schedule many different types of tasks (archiving, aggregation, workflow automation, and so on).
- [\*\*Aliases\*\*](#)  
Create synonyms for a data value or object to be used in reports or queries.
- [\*\*Dates and Timestamps\*\*](#)  
Use a calendar tool to select an exact date, and a relative date picker to select a date that is relative to the current time.
- [\*\*Building Time Periods\*\*](#)  
Policy rules and query conditions can test for events that occur (or not) during user-defined time periods.
- [\*\*Cipher suites\*\*](#)  
Cipher suites are combinations of cryptographic parameters that define the security algorithms and key sizes.
- [\*\*Comments\*\*](#)  
Comments apply to definitions and to workflow process results.
- [\*\*Customer Uploads\*\*](#)  
The Database Protection Subscription Service supports the maintenance of predefined assessment tests, SQL based tests, CVEs, APARs, and groups such as database versions and patches.
- [\*\*Stream Guardium data to another application\*\*](#)  
Use the Data Streaming to send traffic collected by Guardium to another tool for analysis.
- [\*\*Big Data Intelligence\*\*](#)  
The Guardium Big Data Intelligence (GBDI) platform stores collected data over longer timeframes, providing direct, near real-time access to data security and compliance reports and insights.
- [\*\*Exporting and importing definitions\*\*](#)  
Use export and import definitions if you have multiple systems with identical or similar requirements and are not using central management. You can define the components that you need on one system and export those definitions to other systems that are on the same software release level.
- [\*\*Remote loggers\*\*](#)  
View the forwarding rules for the remote logging and test the connections.
- [\*\*Manage Custom Classes\*\*](#)  
Upload and maintain custom classes used in alerts or evaluations. Manage custom classes by clicking Setup > Custom Classes.
- [\*\*GDPR readiness: Considerations when configuring Guardium\*\*](#)  
Learn how Personal Identification Information (PII) data gets stored on your Guardium system, and how to manage this.
- [\*\*Groups\*\*](#)  
Using groups makes it easy to create and manage classifier, policy and query definitions, as well as roll out updates to your S-TAP's and GIM clients. Rather than having to repeatedly define a group of data objects for an access policy, put the objects into a group to easily manage them.
- [\*\*Security Roles\*\*](#)  
Security roles are used to grant access to data (groups, queries, reports, etc.) and to grant access to applications (Group Builder, Query-Report Builder, Policy Builder, CAS, Security Assessments, etc.).
- [\*\*How to install patches\*\*](#)  
Install a single patch or multiple patches as a background process.
- [\*\*Support Maintenance\*\*](#)  
The Support Maintenance feature is password protected and can be used only as directed by Technical Support. Contact Technical Support if you require more information.

## Related information

- [IBM Security Guardium product information](#)

## Guardium Administration

Guardium® administrators perform various administration and maintenance tasks.

Any user assigned the admin role is referred to as a Guardium administrator. The admin role is distinct from the admin user account. The Guardium Administrator role is accountable for the usage of the admin and CLI IDs in production systems.

## Admin role privileges

---

The Guardium admin role has privileges that are not explicitly assigned to that role. For example, when a user with the admin role displays a list of privacy set definitions, all privacy sets defined on the Guardium system display. The user with the admin role can view, modify, or delete any of those definitions. When a user without the admin role accesses the list of privacy sets, that user sees only the following privacy sets:

- The privacy sets that they own (that is, that they created).
- Any privacy sets that are assigned a security role that is also assigned to that user.

Note: If you create a new role that is based on the admin role, any user with the new role has access to the same UI as the admin role. However, the role does not automatically grant access to artifacts created by other users.

## CLI diag command access

---

Use of the **diag** CLI command requires an additional password, which can be the password of any user with the admin role.

If automatic account lockout is enabled (where a user account is locked after a specified number of login failures), the admin user account can be locked after a number of failed login attempts. If that happens, use the **unlock admin** CLI command to unlock it.

Note: The access manager (accessmgr) can unlock accounts from the User Browser. Open the User Browser by clicking Access > Access Management > User Browser.

## Admin user privileges

---

The admin user has extra privileges that are not granted to the admin role, as follows:

- Access to all users' to-do lists
- Owner of imported definitions
- Access management functions

## Admin user To-Do List powers

---

The To-do List is a workflow automation feature that controls the distribution of audit process results to users. The admin user has special privileges and responsibilities in this area. If a user account is disabled, all audit process results for that user are automatically reassigned to the admin user. If a user is unavailable for any other reason, audit process results are installed in that user's to-do list; that is, awaiting sign-off before they are released to the next results receiver. The admin user can open any user's to-do list, and take any actions that are available to that user. When the admin user performs any actions on another user's to-do list, that fact is noted in the audit process activity log, for example, User admin signed results on behalf of user x.

## Imported definition ownership

---

When definitions are exported, all roles are removed, and the owner is changed to the admin user. This is the only way to control how the definition will be used on the importing system.

## Access management and the administrator

---

For security purposes, a separation of duties exists between the access manager and admin. Admin users cannot have access manager privileges, and vice versa.

The next time the admin user logs in, access manager functionality will be available to them. This is possible for the admin user only (and not for other users that have the admin role).

Note:

The same user can contain both of these roles through a legacy situation or as a result of an upgrade. However, current use does not allow the two roles to be assigned to the same user.

In the past, when a unit was upgraded, the accessmgr role was assigned to the admin user, and the accessmgr user was disabled.

In this situation, to configure the accessmgr and admin, log in as admin and enable the accessmgr user, then log in as accessmgr (the default initial password is **guardium**), and remove the accessmgr role from the admin user.

## Certificates

---

Install certificates so you can connect to the Guardium® GUI, and for Guardium-S-TAP communication. Check certificates regularly, so you can update them before they expire.

- [Installing an appliance certificate to avoid a browser SSL certificate challenge](#)

Use Guardium CLI commands to create a certificate signing request (CSR), and to install server, certificate authority (CA), or trusted path certificates on your Guardium system. Installing certificates allows your site to connect to the Guardium GUI without security warnings such as *This site is not secure, or Your connection is not private.*

- [Configuring Guardium-S-TAP communication using an SSL certificate](#)

Create and store an SSL certificate for Guardium-S-TAP communication.

- [Identify expired certificates and certificates that will expire within six months](#)

Expired certificates result in a loss of function. Check certificates regularly to identify certificates that are already expired, and certificates that will expire in the next six months.

- [Managing certificates by using Venafi](#)

Use Venafi to generate and manage GUI, Sniffer, and GIM certificates in your stand-alone or central manager environment.

- [Restoring the Guardium Insights certificate](#)

When you install Guardium, the Guardium Insights self-signed certificate is loaded automatically. If you replace or change that certificate, you can revert to the original certificate by taking the following steps.

## Installing an appliance certificate to avoid a browser SSL certificate challenge

Use Guardium® CLI commands to create a certificate signing request (CSR), and to install server, certificate authority (CA), or trusted path certificates on your Guardium system. Installing certificates allows your site to connect to the Guardium GUI without security warnings such as This site is not secure, or Your connection is not private.

### About this task

For more information about certificate CLI commands, see [Certificate CLI Commands](#).

- You must provide a public certificate from a certificate authority (CA) that you can use to sign your certificates. For example, Verisign, Thawte, Geotrust, GoDaddy, Comodo, or in-house).
- Guardium does not provide CA services and does not ship systems with different certificates other than the default certificate. To use your own certificate, certificate you must contact a third-party CA.
- If the certificate is not self-signed, you must obtain the public certificate for each signer up to the lowest level (for example, that is self-signed). You can use the **openssl x509 -in t.pem -text -nout** command to show contents of a x509 certificate.
- You can obtain and store the public certificate of the CA (step 1) either before or after you generate the CSR (step 2).

### Procedure

1. Have the public certificate from the CA that you need to sign your certificates available.
2. Log in to the CLI and enter the following command:

```
create csr gui
```

Enter the requested information. If the CN (common name) of the certificate is not set to the *hostname.domain* of the system, the browser responds with certificate errors.

Note: If the Common Name (CN=) field starts with a number and is used as an identifier, it must have an *ID:* prefix. For example, **ID:1234**.

You are prompted to supply the organizational unit (OU), country code (C), and so forth. Be sure to enter this information correctly. The last prompt is:

```
What encryption algorithm should be used (1=DSA or 2=RSA) ?
```

The default encryption algorithm is RSA (2). DSA (Digital Signature Algorithm) is a federal information processing standard (FIPS) for digital signatures. RSA is a public-key cryptosystem that involves key generation, encryption, and decryption.

After you select a decryption algorithm, the system displays a description of the request, followed by the request itself, and some additional instructions. For example,

```
Certificate Request:
Data:
Version: 0 (0x0)
Subject: C=US, ST=MA, L=Littleton, O=XYZCorp, OU=Accounting, CN=g2.xyz.com

-----BEGIN NEW CERTIFICATE REQUEST-----
MIICWCCAhcAQAwVDELMakGA1UEBhMCVVMxEDAOBgNVBAgTB1dhbHRoYWoXETAPBgNVBAoTCEd1
YXJkaXVtMRUwEwYDVQQLewxndWFyZG1lb5jb20xCTAHBgNVBAMTADCCAbgwggEsBgcqhkjOOAQb
MIIIBHwKBgQD9f1OBHXUSKVLfSpwu7OTn9hG3UjzvRADDHj+At1EmaUvdQCJR+1k9vj6v8X1ujD2
y5tVbNeB04AdNG/yZmC3a5lQpaSfn+gEexAiwk+7qdf+8Yb+DtX58aophUPBPuD9tFFHsMCNVQT
WhaRMvZ1864rYdcq7/IiAxmd0UgBxwIVAjdguI8VIvwMspK5gqLrhAvvWBz1AoGBAPfhoxWmz3e
y7xrXDa4V7151k+7+jrqgv1XTAs984JnUV1XjrrUWU+mcQc0gYC0SRZxI+hMKBYt88JMozIpue8
FnqLVHyNKOJcrh4rs6Z1kW6jfww6ITVi9ftiegEk08yk8b6oYZCJqIPf4VrlnwaSi2ZegHtVJWQB
TDv+zolkqA4GFAAKBgqCOnSEB4g4/limbHkuZ5Ynl9CGM3a2evEnqjXZts4itxeTYwPqvdkjdSmQ
kaolBxmNUsZOJZrq5nC5Cg3X9spa+BzFr+Pqr/5zka17nHcxKXCjVjLk451l67K11Xv61TUfv/bU
PKmiaGKDttsp2kt4dBFxQdICJEGo0aNFC6qAAMAsGByqGSM44BAMFAAMwADAtAhUAhHTY5z9X
N1BauyaC9PS4Gz1eYakCF2kcfxfjx1bfy5i228XWMAUON95
-----END NEW CERTIFICATE REQUEST-----
```

```

Copy and paste the Certificate Signing Request (CSR), starting at the
'-----BEGIN NEW CERTIFICATE REQUEST-----' tag and ending at the '-----END
NEW CERTIFICATE REQUEST-----' tag, to a file. The CSR file will need to be
provided to a Certificate Authority (CA) of your choice in order to obtain
a valid certificate. Please note that the certificate will need to be in PEM
format so that it can be imported into the Guardium appliance. Once you receive
the certificate from your CA, use the following CLI command to start the import
process:
```

```
<< store certificate gui >>
```

Note:

- For Common Name, enter the hostname in FQDN format (fully qualified domain name). If you connect to the GUI normally using the short hostname (for example, *system1*) instead of the FDQN (*system1.us.ibm.com*), Guardium returns an Address Mismatch certificate error. Either change the CN to use the FDQN, or connect with *https://system1.us.ibm.com:8443/sqlguard* to use the certificate.
- Country Code must be two letters.
- Keysize can be 1024 or 2048.

3. After the CA signs the CSR and returns a signed key, log in to the CLI and enter the following command:

```
store certificate gui console
```

The system returns with the following output:

Please paste your End-Entity certificate below in PEM encoded format. A certificate in PEM encoded format should include the '-----BEGIN CERTIFICATE-----' and '-----END CERTIFICATE-----' tags. The Certificate Authority (CA) Root and Intermediate certificate(s) (if applicable) will also need to be pasted at this time for validation purposes. Please ensure that all certificates are in PEM format and include the aforementioned tags. When pasting multiple certificates, please make sure that each certificate is pasted on a new line in the following order:

```
-----BEGIN CERTIFICATE-----
(End-Entity certificate)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Intermediate certificate(s) - if applicable)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Root certificate)
-----END CERTIFICATE-----
```

Once done pasting your certificate(s), press ENTER followed by CTRL-D to continue.

4. After you load the certificate, the system asks if the certificate matches the existing CSR request.

If you enter yes, the system responds with the following warning: **WARNING: Alias "tomcat" already exists. Are you sure that you want to replace it [y/n]? Enter "y" for yes.**

The system responds with the success or failure of the store operation.

5. Paste the certificate chain together in order, starting with the appliance certificate first and the root certificate last. The GUI restarts automatically. If needed, restart the GUI manually.

## Results

A certificate for one Guardium unit is installed.

## What to do next

Repeat the steps for every Guardium system onsite.

## Configuring Guardium-S-TAP communication using an SSL certificate

Create and store an SSL certificate for Guardium-S-TAP communication.

### About this task

For Windows systems, if you do not choose to use a value for a parameter, do not include it in the guard\_tap.ini. This is pertinent to the CRL path in particular, or if you want to shut off certificate authentication and go back to TLS.

For UNIX or Linux systems, if you do not choose to use a value for a parameter, set its value equal to NULL. This is pertinent to the CRL path in particular, or if you want to shut off certificate authentication and go back to TLS.

Attention: For z/OS, steps [7](#) and [8](#) are not required, but an AT-TLS policy must be configured. Work with your system admins to configure AT-TLS. For more information, see [AT-TLS policy example](#).

## Procedure

1. Log in to the CLI of your Guardium.
2. Enter: `create csr sniffer`
3. Enter the common name (CN) of the requested system to create the CSR request.
4. Get the CSR signed by a certificate authority (CA) service to get the certificate, as well as the root certificate used by the certificate authority (CA) service.  
If the certificate is not already in PEM format, use OpenSSL or another third-party tool to convert it. For example, to convert from PKCS7 format to PEM, use the following OpenSSL command: `openssl pkcs7 -print_certs -in certificate.p7b -out certificate.pem`
5. Store the certificate on your system by entering the CLI command: `store certificate sniffer`
6. If you don't know the CA and the CN of the certificate, enter: `show certificate sniffer`. Output is similar to the following, though the signature algorithm may use a more recent encryption algorithm:

```
Certificate File system.cert.pem
Certificate:
Data:
Version: 1 (0x0)
Serial Number: 12345678912345678999 (0x8ba99886be3317ab)
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=aa, ST=aa, L=aa, O=aa, OU=aa, CN=CYCLOPS
```

7. On the DB server, store the root certificate from certificate authority (CA) service in a file.
8. In the `guard_tap.ini` file, update the following parameters:
  - `guardium_ca_path=[Location of the Certificate Authority certificate]`
  - `sqlguard_cert_cn=<CN from step 3>`
  - `guardium_crl_path=<the path to the certificate revocation list file or directory (the blocklist)>`
9. Restart the S-TAP, and restart the sniffer with the CLI command: `restart inspection-engines`.
10. Verify that the installed certificate is being used by entering `openssl`, for example: `openssl s_client -connect 9.70.157.113:16018`. The output should be similar to  
`-connect 9.70.157.113:16018`  
You are now connected using OpenSSL.

## Identify expired certificates and certificates that will expire within six months

Expired certificates result in a loss of function. Check certificates regularly to identify certificates that are already expired, and certificates that will expire in the next six months.

### About this task

To see a summary of all certificates, run the CLI command **show certificate summary**.

### Procedure

Log in to the CLI and run the command: **show certificate warn\_expire**.

The output lists certificates that will expire within six months and certificates that have already expired.

### Related concepts

- [Certificate CLI Commands](#)

## Managing certificates by using Venafi

Use Venafi to generate and manage GUI, Sniffer, and GIM certificates in your stand-alone or central manager environment.

### About this task

Use the following procedure to integrate your Guardium® stand-alone or centrally managed system with the Venafi certificate management system.

### Procedure

1. Create a Venafi instance. For more information, see [Creating a Venafi instance](#).
2. Configure Venafi for GUI, Sniffer, or GIM certificates. For more information, see [Configuring Venafi for GUI and Sniffer certificates](#), and [Configuring Venafi for GIM certificates](#).
  - **Creating a Venafi instance**  
Set up the Venafi portal to generate signed certificates.
  - **Configuring Venafi for GUI and Sniffer certificates**  
Use the Guardium CLI to configure your Guardium system to connect to Venafi as a Service or TPP instance.
  - **Configuring Venafi for GIM certificates**  
Use the Guardium CLI to configure your Guardium system to connect to the Venafi as a Service or TPP instance.

## Creating a Venafi instance

Set up the Venafi portal to generate signed certificates.

### Procedure

Create user credentials on the Venafi portal and populate the fields in your configuration template. You can optionally use a wildcard in your zone configuration. For more information, see the Venafi documentation.

Tip: Make a note of your zone configuration information. If you are not using a wildcard, you must enter the exact zone configuration information on your Guardium® system to establish a successful connection to Venafi.

## Configuring Venafi for GUI and Sniffer certificates

Use the Guardium® CLI to configure your Guardium system to connect to Venafi as a Service or TPP instance.

### Before you begin

Ensure that Venafi as a Service or TPP instance is configured and running.

### About this task

Use the following procedure to configure GUI or Sniffer certificates.

### Procedure

- If you are using the Venafi TPP instance, store the ROOT CA certificate by running the following command on the central manager or stand-alone system: **store certificate keystore trusted-venafi console** and pasting the Venafi certificate. Skip this step if you are using Venafi as a Service.
- Store the Venafi connection credentials on your Guardium Guardium system by running the CLI command **store certificate cms**.
  - Select 1 to **Add Venafi** to your Guardium system.
  - Enter your Venafi instance type.
  - Select GUI or Sniffer as the type of certificate to install.
  - Enter the authentication type: access token or username and password.
  - For the TPP instance, enter the TPP URL, Venafi token, and the exact zone configuration information that you used when you created your Venafi instance. For Venafi as a Service, enter the zone value and API key. If the information does not match, the connection fails.  
Note: vCert prefixes \VED\Policy\ to the zone. When you enter the zone in the Guardium system, you must specify only the child folders under the root Policy folder.
  - Select enroll or pick up for the vcert action.

**Enroll**  
Use the enroll option to create a new certificate on Venafi and add it to the Guardium keystore.

  - After selecting enroll, if you have custom fields configured on Venafi, add up to nine fields using the **name=value** format.  
Attention: If custom fields are configured as mandatory on Venafi, the names and values must be provided accurately and in the correct format otherwise certificate creation fails.
  - After selecting enroll and defining any custom fields, follow the prompts to enter CN, name of your organization, organization unit, city, state, country code, and optional SANs. This completes the creation of a new certificate on Venafi.

**Pick up**  
Use the pick up option to retrieve certificates manually created on Venafi and add them to the Guardium keystore. Use this option if you do not want to create new certificates through Guardium.
- When prompted, enter **y** or **n** to distribute certificates from the central manager to the managed units, if any. If you enter **y**, propagate the Venafi certificates across your deployment by completing steps [4](#) to [6](#). If you enter **n**, complete only step [4](#).
- Import the GUI or Sniffer certificate into the central manager or stand-alone system:
  - From the CLI, run the command **grdapi venafi\_import variant=[gui|sniffer]**.
  - For GUI certificates, you must restart the GUI by running the CLI command **restart gui**. Sniffer certificates do not require a GUI restart.
  - Run the CLI command **show certificate [gui|sniffer]** to check whether the correct certificate is displayed.
- On the central manager, run the following grdapi commands:  
Important: If the root password on the managed unit doesn't match with the root passkey, you must first reset the root password on the managed unit by running the CLI command **support reset-password root**.
  - Distribute the Venafi configuration files to some or all the managed units: **grdapi export\_config type=venafi host=[all\_managed|group:<group-name>|<IP>|<hostname>] force=[true|false]**
  - Propagate the Venafi ROOT CA certificate to some or all the managed units: **grdapi export\_certificate alias=<alias> host=[all\_managed|group:<group-name>|<IP>|<hostname>] force=[true|false]**  
Note: This command restarts the GUI on the managed unit. Wait until the GUI restarts before you proceed to the next step.
  - Install the Venafi GUI or sniffer certificate on the managed unit: **grdapi venafi\_import variant=[gui|sniffer] api\_target\_host=[all|all\_managed|group:<group-name>|<IP>|<hostname>]**
  - For GUI certificates, you must restart the GUI on the managed units by accessing **Manage > Central Management > Central Management**, selecting the managed units, and clicking **Restart Portal**. Sniffer certificates do not require a GUI restart.
- On each managed unit, run the CLI command **show certificate [gui|sniffer]** to check whether the correct certificate is displayed.

## Configuring Venafi for GIM certificates

Use the Guardium® CLI to configure your Guardium system to connect to the Venafi as a Service or TPP instance.

### Before you begin

Ensure that Venafi as a Service or TPP instance is configured and running.

### About this task

Use the following procedure to configure GIM certificates.

### Procedure

- From the Guardium UI, access **Manage > Module Installation > GIM Global Parameters**. Ensure that the global parameter value for **gim\_auto\_certificate\_distribution** is **1**.
- If you are using the Venafi TPP instance, store the ROOT CA certificate by running the following command on your Guardium system: **store certificate keystore trusted-venafi console** and pasting the Venafi certificate. Skip this step if you are using Venafi as a Service.
- Store the Venafi connection credentials on your Guardium system by running the CLI command **store certificate cms**.
  - Select 1 to **Add Venafi** to your Guardium system.
  - Enter your Venafi instance type.
  - Select **GIM client** as the type of certificate to install.
  - Enter the authentication type: access token or username and password.
  - For the TPP instance, enter the TPP URL, Venafi token, and the exact zone configuration information that you used when you created your Venafi instance. For Venafi as a Service, enter the zone value and API key. If the information does not match, the connection fails.  
Note: vCert prefixes \VED\Policy\ to the zone. When you enter the zone in the Guardium system, you must specify only the child folders under the root Policy folder.
  - Select enroll or pick up for the vcert action.

#### Enroll

Use the enroll option to create a new certificate on Venafi and add it to the Guardium keystore.

- After selecting enroll, if you have custom fields configured on Venafi, add up to nine fields using the **name=value** format.

Attention: If custom fields are configured as mandatory on Venafi, the names and values must be provided accurately and in the correct format otherwise certificate creation fails.

- ii. After selecting enroll and defining any custom fields, follow the prompts to enter CN, name of your organization, organization unit, city, state, country code, and optional SANs. This completes the creation of a new certificate on Venafi.

#### Pick up

Use the pick up option to retrieve certificates manually created on Venafi and add them to the Guardium keystore. Use this option if you do not want to create new certificates through Guardium.

4. If prompted, enter **y** or **n** to distribute certificates from the central manager to the managed units that are GIM servers. If you enter **y**, propagate the Venafi certificates across your deployment by completing steps to [5 to 11](#). If you enter **n**, complete steps [5 to 7](#).
5. Stage the GIM clients with the new certificate by running the CLI command **store certificate gim client venafi**.
  - a. Select the GIM client that is registered to your Guardium system.
  - b. Run the CLI command **show certificate gim client**.
  - c. Select the GIM client to check whether the correct certificate is displayed. The status of the certificate can display as pending, processing, or deployed. You must wait until the certificate is deployed.  
CAUTION:  
Ensure that all your GIM clients are updated with the new certificate. When a new GIM server certificate is stored, a GIM client without the new certificate loses connection to the GIM server.
6. After the GIM client certificate is deployed, run the CLI command **store certificate cms**.
  - a. Select [1](#) to **Add Venafi** to your Guardium system.
  - b. Enter your Venafi instance type.
  - c. Select **GIM server** as the type of certificate to install.
  - d. For the TPP instance, enter the TPP URL, Venafi token, and the exact zone configuration information that you used when you created your Venafi instance.  
For Venafi as a Service, enter the zone value and API key. If the information does not match, the connection fails.
  - e. Follow the prompts to enter CN, name of your organization, organization unit, city, state, country code, and optional SANs.
7. Import a new GIM server certificate by completing the following steps:
  - a. From the CLI, run the command **grdapi venafi\_import variant=gim force=true**.
  - b. Restart the GUI by running the CLI command **restart gui**.
  - c. Run the CLI command **show certificate gim server** to check whether the correct certificate is displayed.  
Note: For authentication to succeed, the GIM server and all related GIM clients must have certificates that are signed by the same CA (root and intermediate, if applicable) for both trusted and private certificates.
8. On the central manager, run the following grdapi commands:  
Important: If the root password on the managed unit doesn't match with the root passkey, you must first reset the root password on the managed unit by running the CLI command **support reset-password root**.
  - a. Distribute the Venafi configuration files to some or all the managed units: **grdapi export\_config type=venafi host=[all\_managed|group:<group-name>|<IP>|<hostname>] force=[true|false]**
  - b. Propagate the Venafi ROOT CA certificate to some or all the managed units: **grdapi export\_certificate alias=<alias> host=[all\_managed|group:<group-name>|<IP>|<hostname>] force=[true|false]**  
Note: This command restarts the GUI on the managed unit. Wait until the GUI restarts before you proceed to the next step.
9. Stage the GIM clients with the new certificate by running the CLI command **store certificate gim client venafi**.
  - a. Select the GIM client that is registered to your Guardium system.
  - b. Run the CLI command **show certificate gim client**.
  - c. Select the GIM client to check whether the correct certificate is displayed. The status of the certificate can display as pending, processing, or deployed. You must wait until the certificate is deployed.  
CAUTION:  
Ensure that all your GIM clients are updated with the new certificate. When a new GIM server certificate is stored, a GIM client without the new certificate loses connection to the GIM server.
10. Complete the following steps on the central manager:
  - a. Import the GIM certificate: **grdapi venafi\_import variant=gim force=true api\_target\_host=[all|all\_managed|host name|IP]**.
  - b. For GUI certificates, you must restart the GUI on the managed units by accessing **Manage > Central Management > Central Management**, selecting the managed units, and clicking **Restart Portal**. Sniffer certificates do not require a GUI restart.
11. Complete the following steps on each managed unit:
  - a. Check whether the GIM server and client are active by running the CLI command **show certificate gim client**. The status of the certificate must change from **deployed** to **active**.
  - b. From the Guardium UI, access **Manage > Module Installation > GIM Process Monitor** and ensure that the connection is active.

## Restoring the Guardium Insights certificate

When you install Guardium, the Guardium Insights self-signed certificate is loaded automatically. If you replace or change that certificate, you can revert to the original certificate by taking the following steps.

### About this task

To learn about the **store system domain** and **store system hostname** system CLI commands referenced in this topic, see [System CLI commands](#).

### Procedure

1. Issue the command for restoring the default certificate:

```
restore default
```

2. Set the domain (**store system domain**) and hostname (**store system hostname**), and then restart the network to set the CN and SAN to FQDN.
3. Ensure that the original Guardium Insights certificate is restored. For more information, see [Domain name and TLS certificates](#).

# Alerts

Learn how to work with alerts.

- [How to create a real-time alert](#)

Send a real-time alert to the database administrator whenever there are more than three failed logins for the same user within five minutes.

- [Notifications](#)

Use the Alerter and Alert Builder to create notifications. When email or other notifications are required for alerting actions, follow this procedure for each type of notification to be defined.

- [Predefined alerts](#)

Guardium comes with a set of predefined alerts that can be found in the Alert Builder.

- [Custom Alerting Class Administration](#)

Use a custom alert class to send alerts to a custom recipient. Upload the custom class, then use the Alert Builder to designate the custom class as an alert notification receiver.

## How to create a real-time alert

Send a real-time alert to the database administrator whenever there are more than three failed logins for the same user within five minutes.

### About this task

Generate real-time security alerts whenever suspicious activity is detected or access policies are violated.

Follow these steps:

1. Create a policy
2. Add rules to the policy
3. Add an action when the rule is triggered
4. Install the policy

Prerequisites

Configure SMTP or SNMP in the Alerter. Open the Alerter by navigating to **Setup** > **Tools and Views** > **Alerter**, and then fill out the SMTP or SNMP information.

Note: Policy violations can also be seen in the Incident Management report.

### Procedure

1. Create a policy.

a. Open the policy builder by navigating to **Protect** > **Security Policies** > **Policy Builder for Data**.

b. Click the icon to create a new policy or modify an existing policy by selecting the policy and clicking the icon.  
c. In the Name and properties panel, select the `Data security policy` type and provide a policy name.

2. Add rules to the policy.

a. Click to open the Rules panel for the policy.

b. Click the icon to add a new rule.

c. In the Rule definition panel, use the Rule type menu to select the `Exception` rule type and use the Rule name field to provide a short descriptive name for the rule.

d. Click to open the Rule criteria panel and define the triggering criteria for the rule.

Use the following settings to create a rule that triggers when there are more than three failed logins for the same user within five minutes:

Under Session level criteria:

- Database user = .

Count each individual database user value separately.

Under SQL criteria:

- Exception type = `LOGIN_FAILED`

Under Other criteria:

- Minimum count = 3

Set the minimum number of times the rule is matched before the action is triggered. The count is reset each time the action is triggered or when the reset interval expires.

- Reset interval = 5

Set the number of minutes after which the rule counter is reset. The counter is also reset when the rule action is triggered.

- Record values = 1 - Log full SQL in policy violation

Define what is included in the policy violation report: no SQL, full SQL, or masked SQL.

Select the Continue to next rule option. Continue testing rules once this rule is satisfied and its action is triggered. If this is not selected, no additional rules are tested after this rule is satisfied.

3. Add an action when the rule is triggered.

a. Click to open the Rule action panel and define actions to take when rule conditions are matched.

b. For this example, select > **ALERT** > **ALERT PER MATCH** to get a notification every time the rule is triggered.

c. From the Add new action window, select a Message template, define a Notification type, and then click OK.

For `MAIL` or `SNMP` notification types, you must configure the alerter at **Setup** > **Tools and Views** > **Alerter**.

d. After defining rule actions, click OK to save the rule definition. Click OK again to save the policy.

4. Install the policy.
  - a. From the Policy Builder for Data, select the policy and then select **Install > Install**.
  - b. From the Install policy window, select the Installation action you want and click **OK**.

Your policy is now installed. Your alert receiver will receive real-time notifications when the policy rules are enacted.

## Notifications

Use the Alerter and Alert Builder to create notifications. When email or other notifications are required for alerting actions, follow this procedure for each type of notification to be defined.

### Alerter configuration

1. Before you choose alerting actions, you must be configure the email SMTP settings in theAlerter
2. Open the Alerter by clicking **Protect > Database Intrusion Detection > Alerter**.
3. Fill out the SMTP and/or SNMP information.
4. After filling out each section, click **Test Connection**, and verify that the connection is working. You will receive a message stating the connection is unreachable if the connection is not working.
5. Click **Apply** to save the configuration.
6. At a minimum, IP Address/Host name, port, and return email address must be specified.
7. Select **Mail** from the Notification Type menu. If the Severity of the message is **HIGH**, the Urgent flag is set.
8. Select a user (which can be an individual or group) from the Alert Receiver list. Additional receivers for real-time email notification are **Invoker** (the user that initiated the actual SQL command that caused the trigger of the policy) and **Owner** (the owner/s of the database). The Invoker and Owner are identified by retrieving user IDs (IP-based) configured by using the Guardium® APIs.
9. Click **Add**.

### Build an alert

1. After configuring the Alerter, open the Alert Builder by clicking **Protect > Database Intrusion Detection > Alert Builder**.
2. Fill out the information in the Settings, Alert Definition, Alert Threshold, and Notification sections and click **Apply**.
3. Choose who will receive the notifications by clicking **Add Receiver..** and choosing a user.

### Predefined alerts

Guardium comes with a set of predefined alerts that can be found in the Alert Builder.

Open the Alert Builder by going to **Protect > Database Intrusion Detection > Alert Builder**. When you open the Alert Builder, you are presented with a list of all existing alerts. Select an alert from the finder and click **Modify** to edit it.

In the Modify Alert page, modify any part of the alert, such as receivers or threshold.

You cannot modify the default queries that the alerts are based on. If you want to modify a query, click the **Edit this Query icon**  for any query to open the Query-Report Builder. Once in the builder, clone any query, and then modify the clone to suit your needs.

After making changes to an alert, click **Apply** to save them.

This table describes all predefined alerts.

Table 1. Predefined Alerts

| Alert                                  | Description                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Active Risky Users - Risky Users Score |                                                                                                                                                                                                                                                                                                                                                     |
| Active S-TAPs Changed                  | Checks for changes to Active S-TAP inspection engines done during the last accumulation interval. The alert will trigger if at least one inspection engine has been changed during the period. By default the alert checks every 1/2 hour and checks the last hour.                                                                                 |
| Aggregation/Arc hive Errors            | Alert once a day on all aggregation or archive tasks that did not complete successfully.                                                                                                                                                                                                                                                            |
| Connection Profiling Alert             | Alert runs every 60 minutes and sends the list of allowed (trusted) connections that were found during the time interval to the Connection Profiling List predefined group.                                                                                                                                                                         |
| CAS Instance Config Changes            | Alert once a day on any CAS instance configuration changes.                                                                                                                                                                                                                                                                                         |
| CAS Templates Changes                  | Alert once a day on any CAS template configuration changes.                                                                                                                                                                                                                                                                                         |
| Data Source Changes                    | Alert once a day on any data source definition changes.                                                                                                                                                                                                                                                                                             |
| Discovered Instances Rules Alert       | Alert when a discovered instance is added or replaced. Displays in the alert builder list as Discovered Instances Rules Alert: Discovered Instance Add or Replace.                                                                                                                                                                                  |
| Database disk space                    | Alert every 10 minutes if internal database is more than 80% filled. For more information about Disk Space (% full) and the Guardium® Nanny process, see <a href="#">Self Monitoring</a> .                                                                                                                                                          |
| Enterprise No Traffic                  | Alert runs only on central manager systems. It is based on a query similar to the query on the No Traffic alert and retrieves the records with: timestamp between X and Y, when X is a query parameter and Y is query from date generated by the alert mechanism based on the accumulation interval (same way the existing no traffic alert works). |

| <b>Alert</b>                                           | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enterprise S-TAPs changed                              | Alert runs on central manager systems only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Failed Logins to Guardium                              | Every 10 minutes alert if there have been more than 5 failed login attempts on the Guardium appliance.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Guardium - Add/Remove Users                            | Alert once a day if any Guardium users have been added or removed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Guardium - Credential Activity                         | Alert once a day if there have been any Guardium credential changes, including LDAP configuration changes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Inactive Managed Unit                                  | Alert runs 30 minutes and sends a notice once a day to the predefined group that is called "Managed Units Alert".                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Inactive S-TAPs Since                                  | Alert once an hour on all S-TAPs that have not been heard from.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Inspection Engines and S-TAP                           | Alert once a day on any activity related to inspection engine and S-TAP configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Investigation Dashboard Issues                         | New issue detected and cannot be resolved automatically                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| No Traffic                                             | Alert to indicate whether there is no traffic from specific database servers. This alert will alert when there is no traffic collected from a server from which the Guardium system was collecting traffic at some point during the last 48 hours. The alert will trigger when there is no traffic within the period defined in the accumulation interval.<br>For example if the accumulation interval is 60 minutes the alert will send an email if there was no traffic from a specific database server in the last hour but there was some traffic in the last 48 hours. The alert will send an email (by default) only every 24 hours. Parameters such as accumulation interval, notification interval, run frequency etc. can be customized. Parameters such as Threshold, Per Line, operator, query etc. should not be changed, as changes to these parameters will cause the alert not to work properly. Note the No Traffic query should not be cloned. |
| No Traffic by Server/Protocol                          | Similar to the regular No traffic alert with the following differences: The alert is per service Name/Net Protocol, and will report per line. There is a new additional parameter: Active Traffic Interval that determines when the last request from each server was received. The alert will trigger under the following conditions: There was No traffic during the alert interval from each server/net protocol but there was traffic since: Active Traffic Interval for that combination.<br>Unlike the regular No traffic alert that will trigger if there was no traffic during the alert interval but there was traffic in the previous 48 hours per server IP.                                                                                                                                                                                                                                                                                         |
| Outlier Analysis Failure                               | Triggered by failure of the outlier mining process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 12.1 and later Outlier with anomaly score 90 and above | Alert once an hour if an outlier with anomaly score 90 and above is encountered.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Policy Changes Alert                                   | Alert once a day if there have been any security policy changes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| QWR Exceptions Alert                                   | Alerts once per session to Syslog if during one hour at least one QWR exception was triggered. The QRW exception occurs when Query Rewrite cannot mask data because the query returns more than 16,000 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Queries Running Long Time                              | Notify if a query takes more than 900 seconds to run.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Scheduled Job Exceptions                               | Alert every 10 minutes on any scheduled job exception (including assessment jobs).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| S-TAP Uninstall Alert                                  | Alerts hourly (default) if an S-TAP is uninstalled from a database server. Alert results are also reported in the S-TAP Uninstall Events report in My Dashboard.<br>Tip: Best practice is to leave the alert settings at their defaults. If you need to change the configuration, run the CLI command <b>restart gui</b> so the changes take effect.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Custom Alerting Class Administration

Use a custom alert class to send alerts to a custom recipient. Upload the custom class, then use the Alert Builder to designate the custom class as an alert notification receiver.

- Before you can use a custom class, you must upload it onto the Guardium system. Click **Setup > Custom Classes > Alerts > Upload Alerting Class** to upload a custom alerting class. Click **Browse** to select a file, then **Apply** to save.
- After uploading the custom class, use it in an alert with the Alert Builder. Open the Alert Builder by clicking **Manage > Database Intrusion Detection > Alert Builder**. Fill out the required information, select **CUSTM** from the Notification Type menu, and click **Save**.

## System performance and monitoring

Learn to use Guardium® tools to maintain system performance: unit utilization reports to identify under- and over-utilized systems; system self-monitoring; and the Services status page.

- [Unit utilization and inspection core performance](#)**

This section presents details about Unit utilization and Buffer usage monitor reports so you can learn to identify problems. It includes troubleshooting tips for queue overflow scenarios, and managing utilization thresholds.

- **Self Monitoring**  
The Guardium solution monitors itself to minimize disruptions and correct problems automatically whenever possible.
- **Services Status panel**  
The Services Status panel is a centralized place to check status of services such as CAS or alerter, and if necessary, investigate each service further. Open the Services Status panel by clicking [Setup > Tools & Views > Services Status](#). Each time the Services Status panel is opened, the status of each service is refreshed.

## Unit utilization and inspection core performance

This section presents details about Unit utilization and Buffer usage monitor reports so you can learn to identify problems. It includes troubleshooting tips for queue overflow scenarios, and managing utilization thresholds.

The Inspection Core (sniffer) is the heart of the Guardium collector. It receives all data that is sent from S-TAPs, Network TAPs, and SPAN ports. It is composed of the following components that perform various tasks of transforming network packets into data that can be stored in the internal MySQL database of the collector:

- Sniffer Engine: The sniffer engine reassembles packets that are coming from a SPAN port or Network TAP, or from S-TAPs that are using the packet capture (pcap) driver to capture data. It is not used to process data that is captured by the native S-TAP drivers, such as KTAP (in the case of UNIX S-TAP).
- Analyzer/Parser: The analyzer determines the database type, protocol, and packet structure that is used for each monitored session. It then passes this information to the Parser, which, as the name implies, parses the SQL statements into their constituent parts (VERB, OBJECT, FIELD, and so on).
- Logger: The parsed data is then passed to the logger, which stores this data into the collector's database.

Each of these inspection core components feature dedicated buffers to cope with temporary spikes in traffic. When these buffers overflow, data loss occurs. When the appliance loses packets, you might notice data missing from Guardium reports or reports with missing fields (such as Database Username). Therefore, managing the performance of the Inspection Core comes down to doing what is necessary to keep the various buffers from overflowing. The most efficient way to do this varies with the size of your Guardium environments.

The sniffer can restart because of logger queue overflow. Any data that is stored in any of the sniffer buffers during a restart is lost.

Open the unit utilization reports by going to [Manage > Reports > Unit Utilization](#), and then selecting one of the reports.

Using aliases is recommended when using unit utilization data in custom and predefined reports. Otherwise, utilization levels display with the values: 1, 2, 3, instead of Low, Medium, High.

- **Buffer usage monitor report**

For environments with up to three collectors, the Buffer usage monitor report is your primary source of information about inspection core performance (although the report is not limited to this information only).

- **Unit utilization and Unit utilization details reports**

The Unit utilization report provides an enterprise-level view of collector usage. It employs a simple Low, Medium, or High indicator that shows which collectors are over or under-used. The analysis is mostly based on Buffer Usage Monitor Data, with a few parameters from the Guardium statistics, collected internally on the collectors. The data is downloaded from the managed collectors. From Unit utilization report, you can click and drill down to see a collector's Unit utilization details report that lists many utilization categories and their levels.

- **Performance issue: buffer usage process not running**

The buffer usage process is running on the system to monitor the sniffer and populate the Buffer usage monitor report. If this process is not running, the report is not populated.

- **Performance issue: analyzer queue overflow**

The logger part of the sniffer has a non-circular buffer that is held in the sniffer memory. If the logger queue increases, the amount of memory used by the sniffer (**mem\_sniffer**) also increases. Once the memory has been used by the sniffer, it is not released until the sniffer restarts. This means that you see the mem\_sniffer value increase as logger queue increases, but never decrease unless the sniffer restarts.

- **Configuring unit utilization data processing**

This procedure describes how to configure Guardium systems for processing and displaying unit utilization data.

## Buffer usage monitor report

For environments with up to three collectors, the Buffer usage monitor report is your primary source of information about inspection core performance (although the report is not limited to this information only).

This report is automatically updated by an internal script every minute, so the information that is contained is the most recent. The script runs on, and populates data for, each appliance individually. By default, the appliance stores two weeks of data.

The Buffer usage monitor report can be used for real-time alerting, correlation alerting, and periodical review for deployment evaluation, trending, and capacity planning for expansion.

The enterprise buffer usage monitor report uses data from the enterprise central manager sniffer buffer usage table.

The Buffer usage monitor report consists of 47 or more columns, most of which you might never use in day-to-day monitoring of the appliance. One of the first things to do is to create a simpler version of this report that contains the following columns:

Table 1. Simplified buffer usage monitor report

| Parameter     | Description                                                                                                                                                    | Interpretation                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Timestamp     | The time the data was collected.                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| % CPU Sniffer | A normalized representation of sniffer CPU usage. For example, 50% sniffer usage on an 8-core appliance means that the sniffer is using 400% CPU (four cores). | % CPU Sniffer can be used as a proxy to identify other problems, or to see if an appliance isn't at its "normal" values, indicating that something changed. For example, often if the sniffer CPU is high the analyzer queue would be higher, meaning the number of flat log requests is high. The number of flat log requests however is a more direct indicator. Higher sniffer CPU can also indicate a change in traffic volume or type. |

| Parameter                   | Description                                                                                                   | Interpretation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|---------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| % CPU Mysql                 | A normalized representation of the running MySQL CPU usage.                                                   | % CPU Mysql can be used as a proxy to identify other problems, or to see if an appliance is not at its "normal" values, indicating something changed. For example, when % CPU Mysql is high the logger queue might be higher, meaning more chance of sniffer restarts. But checking for sniffer restarts is a more direct observation. % CPU Mysql can also be higher due to other non-sniffer processes running on the system like aggregation or audit processes.                                                                                                                         |
| % Memory Mysql              | The percentage of total system memory that is used by the MySQL database.                                     | Provides general background information. This value goes up or down depending on usage of the system. The exact value is not important unless a problem was identified.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Free Buffer Space           | The percentage of free buffer space for the sniffer process.                                                  | The sniffer buffer engine is only used in implementations that use SPAN ports, Network TAPs, or S-TAP PCAP. If the native S-TAP drivers are used, this value usually remains at 100%.                                                                                                                                                                                                                                                                                                                                                                                                       |
| Mem Sniffer                 | Sniffer memory usage in kB.                                                                                   | Sniffer memory usage is always greater than 0 when the sniffer is running. The memory usage increases as more data is held in the logger queue. Memory that is allocated to the sniffer is not released until the sniffer restarts.                                                                                                                                                                                                                                                                                                                                                         |
| Sniffer Process ID          | The sniffer process ID.                                                                                       | The PID value in this column changes when the sniffer restarts.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Analyzer Rate               | An approximate representation of the amount of data that is processed by the Analyzer/Parser per minute.      | The unit of data that is represented is an internal structure that is closely analogous to a packet. The maximum analyzer rate that a specific appliance can handle is a function of several variables, such as the appliance hardware, the type of data that is analyzed and parsed, and the type of rules that are used in the policy. Therefore, analyzer rate alone is not a good indicator of sniffer load, but it can be a good way to identify the busiest times of the day. The Analyzer Rate does not have a generic value that is problematic or a generic 'best practice' value. |
| Analyzer Queue Length       | Indicates the amount of data that is in the Analyzer/Parser buffer.                                           | This value is one of the most direct indicators of sniffer performance. Ideally, the value remains at, or close to, zero. The analyzer queue might grow temporarily during temporary periods of high traffic, but should never remain elevated for more than five or six rows (5 - 6 minutes) in the Buffer Usage Monitor report. The Analyzer/Parser buffer is circular. When the analyzer goes over 80% of queue full, it starts to drop data or put it into flat log, depending on the system configuration. For more information, see <a href="#">Flat log process</a> .                |
| Analyzer Lost Packets (ALP) | Deprecated                                                                                                    | Replaced by <a href="#">Flat log requests</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Logger Rate                 | A rough representation of the amount of data that is processed by the logger per minute.                      | The units here represent the parsed components of the SQL traffic that is inserted into the appliance's internal MySQL database. As with analyzer rate, the logger rate an appliance can handle depends on many factors, such as the appliance hardware, size of SQL statements that are logged, type of policy, and overall load on MySQL imposed by reports, and alerts.                                                                                                                                                                                                                  |
| Logger Queue Length         | The amount of SQL data that is in the logger buffer and waiting to be inserted into the collector's database. | Similar to the analyzer queue, a consistently high amount of data in the logger queue indicates that the appliance is unable to cope with the amount of traffic that is monitored. Temporary spikes in buffered data are normal, provided the buffer is flushed within several minutes.                                                                                                                                                                                                                                                                                                     |
| Session Queue Length        | The total number of open sessions that are monitored by the sniffer.                                          | This information is important because sniffer must allocate a certain amount of memory for each session that is monitored, and it cannot monitor more than 4000 simultaneous sessions.                                                                                                                                                                                                                                                                                                                                                                                                      |
| Session Total               | The overall number of sessions that were opened and closed since the last sniffer restart.                    | Session total can be useful to correlate a spike with other statistics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Mysql Disk Usage            | The Current MySQL disk usage (percentage).                                                                    | High or increasing Mysql disk usage means that the appliance might be in danger of reaching or exceeding 90% full. At that point the sniffer automatically stops. Not related to Inspection Core performance, but should also be included in your simplified Buffer Usage Monitor report.                                                                                                                                                                                                                                                                                                   |
| System CPU Load             | A normalized representation of total system CPU usage.                                                        | System CPU load is derived from % CPU Sniffer and % CPU Mysql, plus other loads on the CPU. Since CPU load is derived from a few measurements, it does not indicate a specific problem. When higher than normal, it can indicate an underlying problem in many areas. Not related to Inspection Core performance, but should also be included in your simplified Buffer Usage Monitor report.                                                                                                                                                                                               |
| Flat Log Requests           |                                                                                                               | <b>Flat log requests indicate that the sniffer is dropping packets.</b> The sniffer usually drops packets due to an analyzer queue overflow problem caused by high traffic. <b>Flat log requests do not increase in a system that is working correctly.</b> If Flat log requests go over the threshold once it is a concern. Flat Log, when configured, takes the overflow from the buffer and stores it in a flat log, then inputs it later to the sniffer, with full analysis according to the policies. For more information, see <a href="#">Flat log process</a> .                     |

## Unit utilization and Unit utilization details reports

The Unit utilization report provides an enterprise-level view of collector usage. It employs a simple Low, Medium, or High indicator that shows which collectors are over or under-used. The analysis is mostly based on Buffer Usage Monitor Data, with a few parameters from the Guardium statistics, collected internally on the collectors. The data is downloaded from the managed collectors. From Unit utilization report, you can click and drill down to see a collector's Unit utilization details report that lists many utilization categories and their levels.

In the Unit Utilization report, each managed collector is displayed with its corresponding utilization level. The three utilization levels are: Low, Medium, and High. Right-click any Guardium system and select Unit Utilization Details to open the Unit Utilization Details report. It provides the statistics and levels of the individual parameters that are used to calculate the overall collector utilization in 1-hour increments over a 24-hour period.

The summary is always per hour. It summarizes the data, starting from the last time it was extracted for each managed unit, until the latest whole hour reported to the central manager. If data was not extracted for a specific unit at all, it starts at 24 hours previous to the current time. For example, data was never extracted for a specific unit and it is now 14:04 on a Tuesday and the latest reported record for that unit has a timestamp Tuesday (today) 13:05. Data is extracted for all whole hours from yesterday (Monday) at 15:00 (now minus 24 hours from the first whole hour). The latest period that is extracted is the period that starts today (Tuesday) at 12:00 (the last whole hour that is reported is between 12:00 and 13:00, since the last record is from 13:05).

The Low, Medium, and High utilization levels are defined by a predefined but configurable set of thresholds. The predefined thresholds are adequate in most cases. Threshold 1 defines the level at which a particular parameter goes from Low to Medium. Threshold 2 defines the level at which a particular parameter is at High utilization. You might see an overall High Utilization level in the Unit Utilization Details report but it might not necessarily be indicative of an issue. If the Guardium system reaches this level for only 1 hour in an extended period, it is most likely an isolated event that can be ignored. If you are getting "too many" false positives, consider modifying the

default thresholds. The rate of false positives is whatever you decide. It might be one per day, or one per week, for example. To modify the thresholds, go to [Manage > Reports > Unit Utilization > Utilization thresholds](#).

The Deployment Health Dashboard, by default, includes a unit utilization issues pane, which is the same as the Unit Utilization Details report.

The two most important statistics in the Unit utilization levels are:

- Number of flat logs: does not increase in a system that is working correctly.
- Number of sniffer restarts: the sniffer does not restart in a system that is working correctly.

These two statistics indicate that data is definitely being dropped. If they go over the threshold once, investigate the reasons. All other statistics can go over thresholds and come back down without actual data loss.

Each measurement has two columns: the hourly statistic, and the level. For example, Number of restarts and Number of restarts level. The hourly statistics are:

Table 1. Unit utilization report

| Parameter                      | Description                                                                                                   | Interpretation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------|---------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hostname                       | Collector or aggregator hostname or IP.                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Period start                   | Hour at which statistics collection started.                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Overall unit utilization level | The highest level from all of the analyzed parameters.                                                        | If the number of sniffer restarts reaches a level of Medium, for example, but all other parameters are Low, the overall Unit utilization level for this period is Medium.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Number of restarts             | Number of times the sniffer restarted.                                                                        | Number of sniffer restarts. <b>Indicates that the sniffer is dropping packets. The sniffer does not restart in a system that is working correctly.</b> If Number of restarts goes over the threshold once, it is of concern. Common causes of sniffer restart: <ul style="list-style-type: none"> <li>• Crash of the sniffer process.</li> <li>• Engine buffers become full.</li> <li>• Logger queues filling up, system out of memory, can be caused by any of:               <ul style="list-style-type: none"> <li>◦ Too much traffic is coming in from the STAPs.</li> <li>◦ High level of traffic is captured by policy rules, for example, Log Full details. (<a href="#">Log full details</a>.)</li> </ul> </li> </ul> |
| Sniffer memory                 | Sniffer memory usage in kB.                                                                                   | Sniffer memory usage is always greater than 0 when the sniffer is running. The memory usage increases as more data is held in the logger queue. Memory that is allocated to the sniffer is not released until the sniffer restarts.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Percent Mysql memory           | The percentage of total system memory that is used by the MySQL database.                                     | Provides general background information. This value goes up or down depending on usage of the system. The exact value is not important unless a problem was identified.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Free buffer space              | The percentage of free buffer space for the sniffer process.                                                  | The sniffer buffer engine is only used in implementations that use SPAN ports, Network TAPs, or S-TAP PCAP. If the native S-TAP drivers are used, this value usually remains at 100%.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Analyzer queue                 | Indicates the amount of data that is in the Analyzer/Parser buffer.                                           | This value is one of the most direct indicators of sniffer performance. Ideally, the value remains at, or close to, zero. The analyzer queue might grow temporarily during temporary periods of high traffic, but should never remain elevated for more than five or six rows (5 - 6 minutes) in the Buffer Usage Monitor report. The Analyzer/Parser buffer is circular. When the analyzer goes over 80% of queue full, it starts to drop data or put it into flat log, depending on the system configuration. For more information, see <a href="#">Flat log process</a> .                                                                                                                                                  |
| Logger queue                   | The amount of SQL data that is in the logger buffer and waiting to be inserted into the collector's database. | Similar to the analyzer queue, a consistently high amount of data in the logger queue indicates that the appliance is unable to cope with the amount of traffic that is monitored. Temporary spikes in buffered data are normal, provided the buffer is flushed within several minutes.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Mysql disk usage               | The Current MySQL disk usage (percentage).                                                                    | High or increasing Mysql disk usage means that the appliance might be in danger of reaching or exceeding 90% full. At that point the sniffer automatically stops.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| System CPU load                | A normalized representation of total system CPU usage.                                                        | System CPU load is derived from % CPU Sniffer and % CPU Mysql, plus other loads on the CPU. Since CPU load is derived from a few measurements, it does not indicate a specific problem. When higher than normal, it can indicate an underlying problem in many areas.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| System var disk usage          | The utilization of the /var partition.                                                                        | Most of files that are generated by the appliance are stored in /var.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Number of requests             | Number of SQL requests that were processed during the time period.                                            | From the internal Guardium statistics. This value is indicative of 'normal' traffic level on the system. The threshold needs to be tuned to the specific environment to be useful.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Number of full SQLs            | Number of full SQL records logged.                                                                            | From the internal Guardium statistics. This value is indicative of 'normal' traffic level on the system. The threshold needs to be tuned to the specific environment to be useful.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Number of exceptions           | Number of exceptions logged.                                                                                  | From the internal Guardium statistics. This value is indicative of 'normal' traffic level on the system. The threshold needs to be tuned to the specific environment to be useful. For example, if there is a massive spike in exceptions on one collector, this might indicate an issue.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Number of policy violations    | Number of policy violations logged.                                                                           | From the internal Guardium statistics. This value is indicative of 'normal' traffic level on the system. The threshold needs to be tuned to the specific environment to be useful. For example, if there is a massive spike in policy violations on one collector, this might indicate an issue.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Number of flat log requests    | Number of requests that were flat logged.                                                                     | <b>Flat log requests indicate that the sniffer is dropping packets.</b> The sniffer usually drops packets due to an analyzer queue overflow problem caused by high traffic. <b>Flat log requests do not increase in a system that is working correctly.</b> If Flat log requests go over the threshold once it is a concern. Flat Log, when configured, takes the overflow from the buffer and stores it in a flat log, then inputs it later to the sniffer, with full analysis according to the policies. For more information, see <a href="#">Flat log process</a> .                                                                                                                                                       |

## Performance issue: buffer usage process not running

The buffer usage process is running on the system to monitor the sniffer and populate the Buffer usage monitor report. If this process is not running, the report is not populated.

## Symptoms

---

Key columns in the Buffer usage monitor report: Timestamp

## Causes

---

A common cause of this is the internal database previously filled up to 90% and the buffer usage process was not restarted afterwards.

## Diagnosing the problem

---

Check the timestamp column of the report and the run time parameters. Does the report have one row every minute up to the current time?

Using the CLI, check if the database is close to full: **support show db-status used %**.

## Resolving the problem

---

If the Buffer usage monitor report does have one row every minute up to the current time, the buffer usage process should be restarted.

If the database is more than 75% full or unusually full for the appliance, consider purging more data. See [Purging data to resolve a full disk when the GUI is down](#).

If the database is at a normal size, restart the buffer usage process.

To restart the buffer usage process, run:

```
restart stopped_services
restart sniffer_buffer_usage
```

Wait 1 minute before checking the reports again.

## Performance issue: analyzer queue overflow

---

## Symptoms

---

Key columns in the Buffer usage monitor report: Analyzer Rate, Analyzer Queue, Flat Log Requests.

You can use **Alerting on Analyzer Queue Overflow** to help identify symptoms.

Analyzer queue is tracked in the [Unit Utilization Level](#) and [Deployment Health View](#). A High status on analyzer queue in these views indicates a likely analyzer queue overflow. You can view the the buffer usage report on the individual collector to confirm.

To alert directly on flat log requests, see [Predefined alerts](#). By default, the alert is set to send to syslog only. Add any receivers that are required. Confirm the alert is active from [Setup > Tools and Views > Anomaly Detection](#).

## Causes

---

There are several reasons for issues with the Analyzer Queue overflowing, but the most common reason is that the sniffer cannot cope with the high rate of traffic that is monitored.

## Diagnosing the problem

---

The analyzer part of the sniffer has a circular buffer. When the queue is full any incoming data is dropped. The amount of dropped data from the last minute is logged in **flat log requests**. If there was data dropped by the analyzer in the last minute, the flat log requests increase. Increasing flat log requests is the key indicator of analyzer queue overflow. For a healthy sniffer it should not be increasing.

## Resolving the problem

---

In the case of high rate of monitored traffic, you must reduce the amount of traffic that is monitored by the appliance by using one of the following strategies:

- Introducing rules to filter more traffic. The most effective rule action to achieve filtering is the Ignore S-TAP Session rule because the sessions are ignored by the S-TAP instead of being sent across the network to the appliance.
- Moving some of the S-TAPs to a less loaded collector
- S-TAP load balancing. Sometimes, a busy database server alone can overwhelm a collector. In these cases, it might help to load balance the traffic from this database to two or more collectors (for more information, see [Linux-UNIX: S-TAP Load Balancing models and configuration guidelines](#) or [Windows: S-TAP Load Balancing models and configuration guidelines](#))
- Consider using a Selective Audit policy. By default, the collector logs all data that is sent to it from S-TAPs or Hardware TAPs. A Selective Audit policy changes this behavior by monitoring only the database traffic that is specified in the policy rules.
- Adding more collectors to the environment.

## Performance issue: logger queue overflow

---

The logger part of the sniffer has a non-circular buffer that is held in the sniffer memory. If the logger queue increases, the amount of memory used by the sniffer (**mem sniffer**) also increases. Once the memory has been used by the sniffer, it is not released until the sniffer restarts. This means that you see the mem sniffer value increase as logger queue increases, but never decrease unless the sniffer restarts.

## Symptoms

---

Key columns in the Buffer usage monitor report: Logger Rate, Logger Queue, Mem Sniffer, Sniffer Process ID.  
When the sniffer restarts the sniffer process ID changes, indicating a new sniffer process has started.

High **logger queue**, and **mem sniffer** reaching its maximum followed by change of **sniffer process ID** means there has been a logger queue overflow problem.

Logger queue overflow is not the only possible cause of sniffer restarts. The sniffer can be restarted from the CLI.

(The logger queue is different from the analyzer queue in that it is not circular and continues to allocate memory until the sniffer reaches 33% of the total system memory.)

You can use **Alerting on Logger Queue Overflow** to help identify symptoms.

Logger queue is tracked in the [Unit Utilization Level](#) and [Deployment Health View](#). A high utilization status on logger queue in these views indicates a likely logger queue overflow. The buffer usage report on the individual collector can then be checked to confirm.

To alert directly on a high number of sniffer restarts, see [Predefined alerts](#). By default, the alert is set to send to syslog only. Add any receivers that are required. Confirm the alert is active from [Setup > Tools and Views > Anomaly Detection](#).

## Causes

---

After the sniffer allocates memory, it does not release it even if the logger queue recovers. Therefore, it is possible to have a high sniffer memory usage even if the logger queues are not holding any data. Sniffer restarts because of logger queue overflow is also shown in the collector's syslog file (/var/log/messages). These messages come in two varieties. The first is a sniffer Memory Allocation Problem, which happens when the logger queues grow quickly. The second type of logger queue overflow restart happens when the Guardium "nanny" process, which monitors sniffer memory usage, detects that the sniffer is dangerously close to the limit and restarts it.

Usually, both types of restarts are caused by the same issues, the only difference being the speed at which the sniffer memory grows. Memory allocation problems happen when the sniffer memory grows quickly before the nanny process can react.

The logger queue can grow for the following reasons:

- Too much traffic or an overly aggressive policy with many heavy rules, such as Log Full Details. Though the solutions for Analyzer Queue issues can also apply here, most times it might be sufficient to reduce the number of Log Full Details or policy violation rules in the policy, or make such rules less inclusive.
- The logger might be competing for MySQL resources if there are an excessive number of reports, correlation alerts, or other internal processes that are running in the background. If your environment includes an Aggregator, consider running daily reports on that appliance instead.

The logger queue is different from the analyzer queue in that it is not circular and continues to allocate memory until the sniffer reaches 33% of the total system memory, by default. This can be configured in the CLI with **support store snif\_memory\_max**.

If the logger queues stay high, the maximum memory is eventually reached. At that point the sniffer automatically restarts and the data in the queues is dropped.

## Resolving the problem

---

Reducing the traffic as for analyzer queue overflow helps to some extent, however the amount of data is not the most common cause of logger queue overflow. Reducing the amount of data logged with intensive logging actions in the policy will have more impact. Sniffer patches are more likely to resolve specific issues leading to high logger queues. Decreasing the workload on the internal database will also improve performance of the logger, for example by running Audit Processes on an aggregator where possible. If the logger queue overflow problem is correlated with a specific scheduled job, that jobs impact on database performance is the likely cause. Suggestions for handling logger queue:

- Install latest sniffer patch from fix central on the appliance
- Reduce amount of traffic logged with 'Log Full Details' or 'Alert per Match' policy actions. See [Configuring your policy to prevent appliance problems](#) for more details.
- Investigate any scheduled jobs that correlate with logger queue overflow.

## Configuring unit utilization data processing

---

This procedure describes how to configure Guardium® systems for processing and displaying unit utilization data.

### About this task

---

For a centrally managed environment, populating the unit utilization information requires scheduling two processes on the central manager: uploading data to the central manager for the buffer usage monitor; and processing the unit utilization data.

For a stand-alone system, you just need to schedule the processing of unit utilization data.

### Procedure

---

1. For a centrally managed environment, define a schedule on the central manager for uploading the central manager buffer usage monitor data.
  - a. Go to Reports > Report Configuration Tools > Custom Table Builder.
  - b. From the Custom Tables screen, select CM Buffer Usage Monitor and click Upload Data to continue.
  - c. From the Upload Data screen, click Modify Schedule to define a schedule for uploading the central manager buffer usage monitor data. Click Save after defining a schedule, then click Back to return to the Upload Data screen.
- Scheduling the process to run once every hour is a reasonable starting point for many deployments, but you may want to adjust the interval around your available resources or data-currency needs.
- Important: To ensure that the most recent data is available for unit utilization reports, define a schedule that processes the buffer usage monitor data before processing the unit utilization data. Additionally, the buffer usage monitor data should not be scheduled to run exactly on the hour.

- Best practice: Define schedules that process the buffer usage monitor data at 10-minutes after the hour and unit utilization data at 40-minutes after the hour.
- From the Upload Data screen, optionally click Run Once Now to immediately upload the data.
2. For a centrally managed environment or for a standalone system, define a schedule for processing unit utilization data.
- In a centrally managed environment, you only need to define the unit utilization schedule on the central manager.
- Go to [Manage > Unit Utilization > Unit Utilization Levels](#).
  - Click Modify Schedule to define a schedule for processing unit utilization data. Click Save after defining a schedule, then click Back to return to the Unit Utilization Levels page.
- Scheduling the process to run once every hour is a reasonable starting point for many deployments, but you may want to adjust the interval around your available resources or data-currency needs.
- Important: To ensure that the most recent data is available for unit utilization reports, define a schedule that processes the unit utilization data after processing the buffer usage monitor data.
- Best practice: Define schedules that process the buffer usage monitor data at 10-minutes after the hour and unit utilization data at 40-minutes after the hour.
- From the Unit Utilization Levels page, optionally click Run Once Now to immediately process the data.

## Results

Go to [Manage > Reports > Unit Utilization](#) to view unit utilization reports. In a centrally managed environment, the data covers the central manager and its managed units. For a standalone system, data is for that individual system. If you did not use the Run Once Now option when defining the schedules, you must wait until those processes run before the unit utilization reports update with the latest data.

## Related information

- [Unit utilization APIs](#)
- [store monitor gdm\\_statistics](#)

## Self Monitoring

The Guardium solution monitors itself to minimize disruptions and correct problems automatically whenever possible.

Guardium uses a three-pronged approach to ensure that it is available, functioning properly, is not been tampered with, and alerts users of problems:

- Reports: Whether textual or graphical, reports are at the core of the Guardium® solution. By using the Guardium Query-Report Builder, a user can effectively report on any of the self-monitoring data that is collected through associated domains and entities. Many of the predefined reports can be enhanced through more detailed effort to provide higher levels of granularity. Use the domain VA Tests to report on tests that are available for security assessments.
- Alerts: In addition to building reports, a user can define an alert against those reports through defined thresholds, indicating an exception or policy rule violation. These alerts can either be real-time or determined through historical analysis. These alerts can then trigger notification to users through SMTP, SNMP, syslog, or a custom Java™ class.
- Self-Monitoring Utility: Guardium has implemented an internal self-monitoring daemon (always running) service utility on collectors and aggregator. This internal self-monitoring daemon wakes up every 5 minutes and does a system scan, checking components for optimal configuration, operational effectiveness, and repairs when necessary. For example, if the utility finds the Web Server down, it first validates a complete shutdown of the service, restarts the service, and then alerts an administrative user.

## Components Monitored

Table 1. Components monitored

| Components                                                                                                                                                                    | How to access                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System                                                                                                                                                                        | Manage > System View > System Monitor                                                                                                                                                                                                                                                                                                                    |
| Disk space(%full)                                                                                                                                                             | Alert: You can use the Queries and Correlation Alerts by using the Sniffer Buffer domain and Sniffer Buffer Usage entity to create alerts                                                                                                                                                                                                                |
| DB sizes and files on disk (/var)                                                                                                                                             | Alerts are sent when the system predicts that a DB size or files on disk (/var) reaches 70% in the next 14 days. Alerts detail the predicted size and the largest tables or files. Alerts are also shown in the deployment health dashboard of the central manager. You can configure and disable the alerts. See <a href="#">Health analyzer APIs</a> . |
| CPU Load<br>Uptime and Reboots<br>Memory Usage<br>Monitoring Engine (sniffer) - Status: up/down/stuck/overloaded<br>CPU Usage<br>Memory Usage<br>Overload and delays (queues) | Reports > Guardium Operational Reports > Buff Usage Monitor<br>Alert: You can use the Queries and Correlation Alerts by using the Sniffer Buffer domain and Sniffer Buffer Usage entity to create alerts                                                                                                                                                 |
| Failed Logins                                                                                                                                                                 | Manage > System View > System Monitor<br>Alert: You can use the Queries and Correlation Alerts, utilizing the Guardium Login domain and Guardium Users Login entity to create alerts                                                                                                                                                                     |

| Components                                | How to access                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Lost requests                             | Manage > Reports > Activity Monitoring > Dropped Requests<br><br>Alert: You can use the Queries and Correlation Alerts by using the Exceptions domain and Exceptions entity to create alerts                                                                                                                                                                                                                                                                                                     |
| Change in data patterns                   | Reports > Real-time Operational Reports > Values Changed<br><br>Alert: See Viewing an Audit Process Definition for alert: Data Source Changes - alert on any data source changes                                                                                                                                                                                                                                                                                                                 |
| Packets rates                             | Reports > Guardium Operational Reports > Buffer Usage Monitor                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Request rates                             | Alert: You can use the Queries and Correlation Alerts by using the Sniffer Buffer domain and Sniffer Buffer Usage entity to create alerts                                                                                                                                                                                                                                                                                                                                                        |
| Ignored data                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Scheduled Jobs<br>Exceptions              | Reports > Guardium Operational Reports > Scheduled Job Exceptions. See <a href="#">Predefined admin reports</a> .<br><br>Alert: You can use the Queries and Correlation Alerts, utilizing the Exceptions domain and Exception Type entity to create alerts.                                                                                                                                                                                                                                      |
| Audit processes status                    | Reports > Guardium Operational Reports > Number of Active Audit Processes. See <a href="#">Predefined admin reports</a> .<br><br>Alert: You can use the Queries and Correlation Alerts, utilizing the Audit Process domain and Audit Process entity to create alerts                                                                                                                                                                                                                             |
| Inspection Engine<br>Changes              | Reports > Activity Monitoring > S-TAP Configuration Change History<br><br>Alert: See Viewing an Audit Process Definition for alert: Inspection Engines and S-TAP - alert on any activity related to inspection engine and S-TAP configuration                                                                                                                                                                                                                                                    |
| Guardium Users Activity<br>- Login/logout | Reports > Guardium Operational Reports > Logins to Guardium, or See Predefined admin Reports<br><br>Alert: You can use the Queries and Correlation Alerts, utilizing the Guardium Login domain and SQL Guard Login entity to create alerts                                                                                                                                                                                                                                                       |
| Failed Logins                             | Reports > Guardium Operational Reports > Logins to Guardium, or See Predefined admin Reports<br><br>Alert: See Viewing an Audit Process Definition for alert: Failed Logins To Guardium - alert if have more than 5 failed logins in the last 11 minutes, or Select Tools > Report Building > drop-down Report Title: Guardium Logins, See Reports for additional information                                                                                                                    |
| User Activity Audit Trail                 | Reports > Guardium Operational Reports > User Activity Audit Trail, or See Predefined admin Reports<br><br>Alert: You can use the Queries and Correlation Alerts, utilizing the Guardium Activity domain and SQL Guard User Activity Audit entity to create alerts<br><br>Note: User activity includes those instances where a user changes to the root shell -- providing a log of their root activity.                                                                                         |
| Creation/Deletion of<br>Users/Roles       | Reports > Guardium Operational Reports > User Activity Audit Trail, or See Predefined admin Reports<br><br>Alert: See Viewing an Audit Process Definition for alert: Guardium - Add/Remove Users - alert on any Addition or Removal of Guardium User                                                                                                                                                                                                                                             |
| Permissions monitoring                    | Reports > Guardium Operational Reports > Guardium Users, Guardium Roles, or Guardium Applications<br><br>Alert: You can use the Queries and Correlation Alerts, utilizing the Application domain and Application Data entity to create alerts                                                                                                                                                                                                                                                    |
| S-TAP Info (Central<br>Manager)           | Report: See S-TAP Reports. On a Central Manager, an additional report, S-TAP Info, is available. This report monitors S-TAPs of the entire environment. Upload this data using the Custom Table Builder. This report is the result of uploading data using remote sources on a Central Manager and using that data to see a consolidated view of S-TAPs.<br><br>S-TAP info is a predefined custom domain which contains the S-TAP Info entity and is not modifiable like the entitlement domain. |

## Guardium nanny process

The Guardium nanny is an internal process that monitors key components and critical resources within the Guardium system—guaranteeing their availability and reliability. The nanny alerts when potential problems are emerging. Nanny alerts go to syslog, can be forwarded and sent as emails to the administrator. In some cases the nanny can take remedial actions.

The monitored resources and components include:

- Web service monitoring - service port (default 8443) not responding or tomcat service is not up
  - syslog message
  - mail admin
  - will issue restarts of the web service
- Inspection Engine activity - snif overloaded, not responding, or failure
  - syslog message
  - mail admin
  - mail guardium support (optional)
  - tries to fix by restarting the snif under certain conditions
  - tries to respawn snif if process dies
- Diskspace utilization - alerts when > 75% on the critical partitions
  - syslog message
  - alert admin
  - performs preventive action by cleaning temporary files when over 95%
- Monitor internal database (TURBINE) - verify service is up, status, and capacity utilization monitoring
  - syslog message
  - mail admin
  - restart service
- File System utilization - every five minutes, Nanny.pl checks file system at /var, warning alert when > 75% in the /var directory, critical alert and services stopped when >90% in /var directory
  - syslog message
  - alert admin
  - Admin clean-up required, using CLI commands: show filesystem usage, clear filesystem dir, and restart stopped\_services
- remote syslog. You can send test messages to the rsyslog to verify that it is communicating with Guardium. To enable and configure the rsyslog test, use the API command [modify\\_guard\\_param](#). To run the test, use the CLI command [show remotelog status](#).
  - If the test message is successful, the response is success.

- If the test message is unsuccessful, Guardium restarts the rsyslogd and checks with a test message. If the test message is successful, the response is success.

- **Monitoring with SNMP**

An SNMP agent is installed on Guardium systems, and read-only access is provided using the SNMP community name of **guardiumsnmp**. You can use SNMP commands within Guardium to display SQL Guard SNMP information.

- **Running Query Monitor**

The Running Query Monitor displays the status of active user queries, and enables you to set a timeout value for all Report/Monitor queries.

## Related information

---

- [Troubleshooting the internal database](#)

## Monitoring with SNMP

---

An SNMP agent is installed on Guardium® systems, and read-only access is provided using the SNMP community name of **guardiumsnmp**. You can use SNMP commands within Guardium to display SQL Guard SNMP information.

When querying, a value of -1 (minus one) indicates a NULL in the database. The table at the end of this section lists the available SNMP OIDs.

## SNMP Examples

---

From a Unix session, you can display SQL Guard SNMP information using the **snmpget** or **snmpwalk** commands. For more information about the **snmpget** and **snmpwalk** commands, call **snmpget -h** or **snmpwalk -h**. Various UI-based software packages are available to display SNMP information. Those alternatives are not described here.

Note: For version 3 SNMP commands, the securitylevel depends on how the SNMP user is created. On the Guardium appliance, you must set securitylevel to *authPriv*. For *authPriv*, you must provide an authentication type, encryption type, authentication password and encryption password.

Table 1. SNMP 3 examples

| SNMP Examples                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>snmpget -v 3 -u SNMPV3USER -a MD5 -A password -x AES -X password -l authPriv 9.42.101.8 UCD-SNMP-MIB::dskAvail.1</code>                                                                                                                                                                                                       |
| <code>snmpget -v 3 -u SNMPV3USER -a MD5 -A password -x AES -X password -l authPriv 9.42.101.8 UCD-SNMP-MIB::dskUsed.1</code>                                                                                                                                                                                                        |
| List total memory and used memory:                                                                                                                                                                                                                                                                                                  |
| <code>snmpget -v 3 -u SNMPV3USER -a MD5 -A password -x AES -X password -l authPriv 9.42.101.8 HOST-RESOURCES-MIB::hrStorageSize.1</code>                                                                                                                                                                                            |
| <code>snmpget -v 3 -u SNMPV3USER -a MD5 -A password -x AES -X password -l authPriv 9.42.101.8 HOST-RESOURCES-MIB::hrStorageUsed.1</code>                                                                                                                                                                                            |
| List the available memory:                                                                                                                                                                                                                                                                                                          |
| <code>snmpwalk -v 3 -u SNMPV3USER -a MD5 -A password -x AES -X password -l authPriv 9.42.101.8 UCD-SNMP-MIB::memAvailReal.0</code>                                                                                                                                                                                                  |
| List values relating to CPU usage:                                                                                                                                                                                                                                                                                                  |
| <code>snmpwalk -v 3 -u SNMPV3USER -a MD5 -A password -x AES -X password -l authPriv 9.42.101.8 ssCpuRawUser</code>                                                                                                                                                                                                                  |
| <code>snmpwalk -v 3 -u &lt;user name&gt; -a &lt;authenticator type &lt;MD5 SHA&gt;&gt; -A &lt;authentication password&gt; -x &lt;encryption type &lt;AES DES&gt;&gt; -X &lt;encryption password&gt; -l &lt;securityLevel &lt;authNoPriv   AuthPriv   noauthNoPriv&gt;&gt; &lt;server with snmp v3 enabled&gt; ssCpuRawSystem</code> |
| <code>snmpwalk -v 3 -u SNMPV3USER -a MD5 -A password -x AES -X password -l authPriv 9.42.101.8 ssCpuRawSystem</code>                                                                                                                                                                                                                |
| <code>snmpwalk -v 3 -u &lt;user name&gt; -a &lt;authenticator type &lt;MD5 SHA&gt;&gt; -A &lt;authentication password&gt; -x &lt;encryption type &lt;AES DES&gt;&gt; -X &lt;encryption password&gt; -l &lt;securityLevel &lt;authNoPriv   AuthPriv   noauthNoPriv&gt;&gt; &lt;server with snmp v3 enabled&gt; ssCpuRawNice</code>   |
| <code>snmpwalk -v 3 -u SNMPV3USER -a MD5 -A password -x AES -X password -l authPriv 9.42.101.8 ssCpuRawNice</code>                                                                                                                                                                                                                  |
| <code>snmpwalk -v 3 -u &lt;user name&gt; -a &lt;authenticator type &lt;MD5 SHA&gt;&gt; -A &lt;authentication password&gt; -x &lt;encryption type &lt;AES DES&gt;&gt; -X &lt;encryption password&gt; -l &lt;securityLevel &lt;authNoPriv   AuthPriv   noauthNoPriv&gt;&gt; &lt;server with snmp v3 enabled&gt; ssCpuRawIdle</code>   |
| <code>snmpwalk -v 3 -u SNMPV3USER -a MD5 -A password -x AES -X password -l authPriv 9.42.101.8 ssCpuRawIdle</code>                                                                                                                                                                                                                  |

Table 2. SNMP 2c examples

| SNMP Examples                                                                                                                                                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Display used and available disk space :                                                                                                                             |
| <code>&gt; snmpget -v 2c -c guardiumsnmp a1.corp.com UCD-SNMP-MIB::dskAvail.1</code><br>UCD-SNMP-MIB::dskAvail.1 = INTEGER: 1043856                                 |
| <code>&gt; snmpget -v 2c -c guardiumsnmp a1.corp.com UCD-SNMP-MIB::dskUsed.1</code><br>UCD-SNMP-MIB::dskUsed.1 = INTEGER: 914856                                    |
| List total memory and used memory:                                                                                                                                  |
| <code>&gt; snmpget -v 2c -c guardiumsnmp a1.corp.com</code><br>HOST-RESOURCES-MIB::hrStorageSize.101<br>HOST-RESOURCES-MIB::hrStorageSize.101 = INTEGER: 2067352    |
| <code>&gt; snmpget -v 2c -c guardiumsnmp a1.corp.com</code><br>HOST-RESOURCES-MIB::hrStorageUsed.101<br>HOST-RESOURCES-MIB::hrStorageUsed.101 = INTEGER:<br>1017548 |
| List the available memory:                                                                                                                                          |
| <code>&gt; snmpwalk -v 2c -c guardiumsnmp a1.corp.com memAvailReal</code><br>UCD-SNMP-MIB::memAvailReal.0 = INTEGER: 1049564                                        |
| List values relating to CPU usage:                                                                                                                                  |
| <code>&gt; snmpwalk -v 2c -c guardiumsnmp a1.corp.com ssCpuRawUser</code><br>UCD-SNMP-MIB::ssCpuRawUser.0 = Counter32: 89240                                        |

| <b>SNMP Examples</b>                                                                                              |
|-------------------------------------------------------------------------------------------------------------------|
| > snmpwalk -v 2c -c guardiumsnmp a1.corp.com ssCpuRawSystem<br>UCD-SNMP-MIB::ssCpuRawSystem.0 = Counter32: 195310 |
| > snmpwalk -v 2c -c guardiumsnmp a1.corp.com ssCpuRawNice<br>UCD-SNMP-MIB::ssCpuRawNice.0 = Counter32: 11         |
| Note: Adding the RawUser, RawSystem, and RawNice numbers provides a good approximation of total CPU usage.        |
| > snmpwalk -v 2c -c guardiumsnmp a1.corp.com ssCpuRawIdle<br>UCD-SNMP-MIB::ssCpuRawIdle.0 = Counter32: 26734332   |

## Guardium SNMP OID

Table 3. Guardium SNMP OID

| <b>SNMP OID</b>                                                  | <b>Description</b>                                                                                 |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| .1.3.6.1.4.1.2021.9.1.7.1<br>UCD-SNMP-MIB::dskAvail.1            | Disk space available in / directory                                                                |
| .1.3.6.1.4.1.2021.9.1.7.2<br>UCD-SNMP-MIB::dskAvail.2            | Disk space available in /var directory                                                             |
| .1.3.6.1.4.1.2021.9.1.8.1<br>UCD-SNMP-MIB::dskUsed.1             | Disk space used in / directory                                                                     |
| .1.3.6.1.4.1.2021.9.1.8.2<br>UCD-SNMP-MIB::dskUsed.2             | Disk space used in /var directory                                                                  |
| .1.3.6.1.2.1.25.2.3.1.5.1<br>HOST-RESOURCES-MIB::hrStorageSize.1 | Total memory available                                                                             |
| .1.3.6.1.2.1.25.2.3.1.6.1<br>HOST-RESOURCES-MIB::hrStorageUsed.1 | Memory in use                                                                                      |
| .1.3.6.1.4.1.2021.8.1.101.1<br>UCD-SNMP-MIB::extOutput.1         | Open monitored session count                                                                       |
| .1.3.6.1.4.1.2021.8.1.101.2<br>UCD-SNMP-MIB::extOutput.2         | Requests logged by the current sniffer process (set to zero for each restart)                      |
| .1.3.6.1.4.1.2021.8.1.101.3<br>UCD-SNMP-MIB::extOutput.3         | Last session timestamp                                                                             |
| .1.3.6.1.4.1.2021.8.1.101.4<br>UCD-SNMP-MIB::extOutput.4         | Last construct timestamp                                                                           |
| .1.3.6.1.4.1.2021.8.1.101.5<br>UCD-SNMP-MIB::extOutput.5         | Memory used by the sniffer process                                                                 |
| .1.3.6.1.4.1.2021.8.1.101.7<br>UCD-SNMP-MIB::extOutput.7         | Packets in on ETH1/ out on ETH2; usually only one number (inbound) when a SPAN port or TAP is used |
| .1.3.6.1.4.1.2021.8.1.101.8<br>UCD-SNMP-MIB::extOutput.8         | Packets in on ETH3/ out on ETH4; usually only one number (inbound) when a SPAN port or TAP is used |
| .1.3.6.1.4.1.2021.8.1.101.9<br>UCD-SNMP-MIB::extOutput.9         | Packets in on ETH5/ out on ETH6; usually only one number (inbound) when a SPAN port or TAP is used |

Other MIBs accessible in the machine are: SNMPv2-MIB, IF-MIB, RFC1213-MIB, and HOST-RESOURCES-MIB.

## Running Query Monitor

The Running Query Monitor displays the status of active user queries, and enables you to set a timeout value for all Report/Monitor queries.

Open the Running Query Monitor by clicking [Manage](#) > [Activity Monitoring](#) > [Running Query Monitor](#).

From the Running Query Monitor, you can:

- Set the query timeout for all reports and monitors that are running in a portlet. Other query processes, such as policy simulations, audit processes, and internal processes are not affected by this timeout value. The default is 180 seconds (3 minutes).
- Kill any currently running user query. Some queries that are listed in this panel—audit processes, for example—can exceed the query timeout specified. That is expected, because the Report/Monitor query timeout applies only to reports and monitors running in a portlet.

We do not recommend setting the Query Timeout higher than the default setting (180 seconds) for an extended time. If you set this limit higher, it increases the chances of overloading the system with ad-hoc reporting activity.

To change the timeout setting, type a number of seconds in the Report/Monitor Query Timeout (seconds), and click Update. You will be informed when the update finishes.

## Services Status panel

The Services Status panel is a centralized place to check status of services such as CAS or alerter, and if necessary, investigate each service further. Open the Services Status panel by clicking **Setup > Tools & Views > Services Status**. Each time the Services Status panel is opened, the status of each service is refreshed.

Say that you set up a policy that sends a real-time alert whenever there are more than three failed log-ins in 5 minutes. To protect against this possible intrusion, you must make sure that the policy was installed, and that the alerter is on.

Use the Services Status panel to verify that both of these services are configured properly.

Clicking any service takes you to its configuration page, where you can, as relevant, turn the service off or on, restart a service, configure a service, etc.

If for some reason the policy didn't install correctly, click **Setup > Tools & Views > Policy Installation** to go to Policy Installer, view the currently installed policies, and make the necessary changes.

Each service displays one of the following icons:

- Service is running/scheduled: 
- Service is paused: 
- Service is off: 

## Scheduling

The general-purpose scheduler is used to schedule many different types of tasks (archiving, aggregation, workflow automation, and so on).

Depending on the type of task being performed, not all of the features described here might be available - for example, the schedules for some types of tasks can be paused, while others cannot be (they can only be stopped or started).

Note: Be aware of scheduling anomalies that might occur when scheduling tasks during Daylight Saving Time.

## Define or Modify a Schedule

1. Access the Scheduling pane from the specific task.
2. Schedule by:
  - Day: select the days.
  - Month: select either the day of the month, or the day of the week; and either every month or specific months.
3. If you want the task to run more than once per day, define the repeat schedule by specifying the interval (in hours) between the tasks. You can also define it to run more than once per hour.  
Note:  
When the schedule is defined to repeat multiple times within an hour, the iteration starts and ends within the hour. The next hour is considered as a new iteration.  
For example, if a job is scheduled to run every 15 minutes starting at 12:15 PM, the job runs at 12:15 PM, 12:30 PM, and then at 12:45 PM. The next iteration begins at 1:15 PM and runs again at 1:30 PM and 1:45 PM.  
To run a job 4 times within an hour, schedule the job to begin before the first quarter of the hour. For example, a job that is scheduled to begin at 12:05 PM repeats at 12:20 PM, 12:35 PM, and 12:50 PM. The next iteration begins at 1:05 PM.
4. Fill in the Start Schedule at. This is the hour at which the schedule starts.
5. In the Begin Schedule, enter the date and time at which the task should first run. If you choose a date earlier than the current date, it reverts to the current date.
6. Select Activate Schedule if activate the schedule.
7. Optionally, select Auto run dependent jobs to automatically find all the job's prerequisite jobs and run them in order, before running this job. This ensures that the job runs with the latest, most accurate data.
8. Click Save. If you selected Auto run dependent jobs, a popup opens with details of the prerequisite jobs that must execute just before this job runs. For more information, see [Job dependencies](#).

## Pause a Schedule

Note: Not all types of scheduled tasks provide a pause option.

1. Clear Activate schedule and save the job.
  - [Job dependencies](#)  
When you create and schedule tasks such as installing policies, updating groups, or running audit processes, you can run the task on a schedule that you define for that process. If that task (the parent) depends on other scheduled jobs (such as jobs that populate groups that are needed by the audit process), then the schedule must ensure that related jobs run and complete in a timely manner before the parent task starts.
  - [Viewing job history](#)  
The job history view provides a Gantt chart that shows when jobs ran and for how long. The chart supports audit, aggregation, and data mart jobs and includes information about start and stop times, duration (current, shortest, longest, and average), and task count.

## Job dependencies

When you create and schedule tasks such as installing policies, updating groups, or running audit processes, you can run the task on a schedule that you define for that process. If that task (the parent) depends on other scheduled jobs (such as jobs that populate groups that are needed by the audit process), then the schedule must ensure that related jobs run and complete in a timely manner before the parent task starts.

Manually defining a schedule that includes these dependent jobs can be complicated or impossible. Therefore, to automate the process, select Auto-complete dependent jobs, which takes the following steps:

1. Guardium checks to see whether the parent task has dependent jobs.

Note: This is a specific check: For example, if the parent task depends on a group, and the group is populated by a query, the query that populates the group must run first to refresh the group (that is, the parent task depends on the group). However, if that group is static or not populated by a query, then the parent task does not have a dependency on the group. In this case, it is your responsibility to ensure that the data in the group is up to date.

- If dependent jobs are found, Guardium checks to see whether the jobs have run in the past 24 hours.
- If the dependent jobs have not run in the past 24 hours, Guardium runs the dependent jobs in the appropriate order. That is, if dependent jobs have dependencies on each other, they are run sequentially and in an order that clears those dependencies.

2. After all of dependent jobs run successfully, the parent job runs.

3. If any of the dependencies fails to run, the job that is currently scheduled does not run. If a failure occurs, an error message is written to the Scheduled Jobs Exception report. The dependent job will retry three times, three minutes apart before failing.

Guardium has defined dependencies for several different job types.

Table 1. Job dependencies. When Auto-complete dependent jobs is selected, Guardium manages job dependencies for the described situations.

| Job type                                                | Dependent jobs                                                                                                                                                                                                                                                                  | Reason                                                                                                                                     |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Audit process with discover sensitive data task         | Where the task includes a discover sensitive data scenario with a Policy >_Rule_>_Action for Add To Group of Objects, Add To Group of Object/Fields or Add To Access Rule. For more information, see <a href="#">Discovery scenarios</a> and <a href="#">What to discover</a> . | Before installing policy rules that use groups, the group data must be up to date.                                                         |
| Audit Process with report task                          | A custom table upload job where the custom table name is referred to by the report audit task.                                                                                                                                                                                  | Custom table data that is referred to by a report-type audit task must be populated with up-to-date data before the Audit Process can run. |
| Audit Process with report task                          | Groups that are defined in an audit task report condition that are populated by the 'Populate From Query' mechanism.                                                                                                                                                            | Groups that are referred to by a query condition must be populated with up-to-date data before a report-type Audit Task can run.           |
| Audit Process (for aggregators)                         | Import                                                                                                                                                                                                                                                                          | For aggregators only. Ensures that information is imported from all aggregated units before any audit process can run.                     |
| Policy Installation with a discover sensitive data task | Groups that are defined in any policies to be installed that are populated by the 'Populate From Query' mechanism.                                                                                                                                                              | Before installing policy rules that use groups, the group data must be up to date.                                                         |
| Populate From Query                                     | Populating a query that uses an uploaded custom table as an entity.                                                                                                                                                                                                             | For any entity that uses populate from query with custom table data, the custom table must be populated with up-to-date data.              |

To enable job dependencies, select Auto run dependent jobs in the Scheduler of a task. When you save the task, a window opens with details of the prerequisite jobs that must run before this job runs.

To identify job dependencies, run the [auto\\_execute\\_suggested\\_dependencies](#) API with the jobTrigger=<job name> parameter.

To obtain a list of all the scheduled jobs and triggers, run the [list\\_scheduler\\_jobs](#) API.

## Related concepts

- [External data correlation](#)

## Related reference

- [Schedule and dependencies APIs](#)

## Viewing job history

The job history view provides a Gantt chart that shows when jobs ran and for how long. The chart supports audit, aggregation, and data mart jobs and includes information about start and stop times, duration (current, shortest, longest, and average), and task count.

## Before you begin

The job history chart does not show jobs that ran for less than 1 minute and does not show failed or canceled jobs.

## Procedure

1. Open Investigate > Job History.
2. Optional: Define a time period for the chart.  
The default period is two weeks, including the current date.
  - a. Click the  icon to open the Specify time period dialog.
  - b. Use the Period start and Period end controls to define a time period.
  - c. Click OK to apply the settings.
3. Review the job history.  
Jobs are listed vertically on the y-axis while time is shown horizontally on the x-axis. Job duration is indicated by the length of horizontal bars that represent individual jobs.
4. Investigate specific jobs.
  - a. Hover on individual jobs to see details.  
Depending on the specific job, the details can include start and stop times, duration (current, shortest, longest, and average), and task count.
  - b. For jobs with tasks, click the job to see individual tasks and task durations.

# Aliases

Create synonyms for a data value or object to be used in reports or queries.

## Aliases Overview

Aliases display a meaningful or user-friendly name for a data value.

For example, *Financial Server* might be defined as an alias for IP address 192.168.2.18. After you define an alias, users can display report results, formulate queries, and enter parameter values with the alias instead of the data value.

Aliases can be defined in a number of ways:

- Through the IP-to-Hostname Aliasing tool - use this tool to generate aliases for discovered client and server IPs.  
Click **Protect > Database Intrusion Detection > IP-to-Hostname Aliasing** to open the IP-to-Hostname Aliasing tool.
- Through the Alias Builder - use this method to define aliases manually.  
Open the Alias Builder by clicking **Comply > Tools and Views > Alias Builder**.
- Through a GuardAPI or REST API query.
- Through the Alias Quick Definition while using the Group Builder pane.

Note: Alias changes on the Central Manager or managed units are not available on other systems until either GUI is restarted or any alias changes are made through their GUI.

## IP-to-Hostname Aliasing

One of the more common applications of aliases is to use them as synonyms for IP addresses. Use this tool to schedule the discovery of client and server IP's and generate aliases for them.

1. Open the IP-to-Hostname Aliasing tool by clicking **Protect > Database Intrusion Detection > IP-to-Hostname Aliasing**.
2. Check the Generate Hostname Aliases for Client and Server IPs (when available) check box.
3. Check the Update existing Hostname Aliases if rediscovered check box if you want the tool to continually look for and update hostname aliases.
4. Click **Apply** to save your configuration, then schedule the operation.
  - Click **Run Once Now** to start the tool immediately.
  - Click **Define Schedule...** to schedule the tool in the future.
  - Click **Pause** to pause the generation of client and server IPs aliases.

## Alias Builder

Use this method to manually create an alias.

1. Open the Alias Builder by clicking **Setup > Tools and Views > Alias Builder**.
2. Select the attribute type for which you want to define aliases.
3. Filter your search on that attribute type that uses the Value and Alias fields and click **Search**.
4. If any results match your search, they display in the value and alias table. Click **Apply** for the search results, or add a new alias by specifying a Value and Alias name, then clicking **Add**.
5. Add a comment to an alias by clicking the Item Comments icon . Comments can be helpful for quickly referencing what an alias refers to in the future.

## Define Aliases using a Query

Use this method to create aliases from a query. When a custom table is uploaded to Guardium®, that table is available to map aliases to specific values.

Restriction:

- When importing group members from Members tab > Import From query using Run Once Now, the maximum number of imported members is 5,000 rows. This is not configurable.
- When importing group members from Members tab > Import From query using a schedule, the maximum number of imported members is 20,000 rows by default. You can configure this limit with the CLI command **show/store populate\_from\_query\_maxrecs**. For more information, see [Configuration and Control CLI Commands](#).

1. Open the Alias Builder by clicking **Setup > Tools and Views > Alias Builder**.
2. Select the attribute type for which you want to define aliases from the Alias Finder and click **Populate from Query** to open the Builder Alias From Query Set Up pane.
3. Enter the required information and click **Save** to save the alias.
  - Select the query to run from the Query menu.
  - Choose a value for both Choose Column for Value Column and Choose Column for Alias Column.
  - After you select column values, more fields display that require input (From Date, To Date, Remote Source, and any additional parameters for the selected query).
  - Check the Clear existing group members before Importing check box to delete the existing content of the group before you populate from the query.
  - Click **Save** to save.
  - With the query saved, the Scheduling buttons become active. Click **Modify Schedule** to run the query in the future, or click **Run Once Now** to run it immediately.

## Alias Quick Definition from Group Builder

Use this method to create an alias for a group immediately when you create or populate a group.

1. Open the Group Builder by clicking **Setup** > **Group Builder**. Select any group from the list, and click **Modify**.
2. Click **Aliases** to open the Alias Quick Definition window. Type in an alias for any group or groups, and click **Apply** to save the alias.

## Related reference

---

- [create\\_alias](#)
  - [delete\\_alias](#)
  - [list\\_aliases](#)
  - [update\\_alias](#)
- 

## Dates and Timestamps

Use a calendar tool to select an exact date, and a relative date picker to select a date that is relative to the current time.

There are two tools that Guardium provides to populate date fields: a calendar tool to select an exact date, and a relative date picker to select a date that is relative to the current time (now -1 day, for example). In addition, you can manually enter exact or relative dates.

Note: When you select or enter dates, the date on the system on which you are running your browser might not be the same as the date on the Guardium® appliance to which you are connected.

### Timestamps in Queries

---

Be careful when you include Timestamps in queries.

First, be aware of the distinction between a timestamp (lowercase t) and a Timestamp (uppercase T).

- A timestamp (lowercase t) is a data type containing a combined date-and-time value, which when printed displays in the format yyyy-mm-dd hh:mm:ss (for example, 2020-07-17 15:40:25). When you create or edit a query, most attributes with a timestamp data type display with a clock icon in the Entity List pane.
- A Timestamp (uppercase T) is an attribute that is defined in many entity types. It usually contains the time that the entity was last updated.

Including a Timestamp attribute value in a query produces a row for every value of the Timestamp, which can produce an excessive amount of output. Instead, use the count aggregator when including the Timestamp in a query, and then drill down on a report row to view the individual Timestamp values for the items included in that row only, in a drill-down report. See **Aggregate Fields in Queries**.

When displaying a Timestamp value in a query that contains Timestamp attributes in multiple entities, be careful to select the Timestamp attribute from the appropriate entity type for the report. For example, if the query displays information from both the client/server and the Session entities, with the Session selected as the main entity, you can display a Timestamp attribute from one or both entities. If you include the client/server Timestamp, you see the same value printed for every Session for a given client/server connection – always the time at which that particular client/server was last updated. If you include the Timestamp attribute from the Session, you see the time that each Session listed was last updated.

Tip: If your report displays the same times when you expect them to be different, the report probably includes a Timestamp attribute from an entity too high in the entity hierarchy for the level of detail you want on the report.

### Select an Exact Date from Calendar

---

To use the Calendar Window to select an exact date:

1. Click **Calendar** for the field where you want to insert a date. The calendar opens in a separate window.
  - Click the arrows to display the previous or next month in the calendar window.
2. Click any date to select that day. The calendar window closes and the selected date is inserted into the date field next to the calendar tool that you clicked.

Note: The default time for a date that is selected from the calendar is always 00:00:00 (midnight). To specify a different time, enter the time that you want in 24-hour format: hh:mm:ss, where hh is the hour (0-23), and mm and ss are minutes and seconds (both 0-59).

### Enter an Exact Date Manually

---

1. Click the field where you want to enter the date and enter the date in YYYY-MM-DD format, where:
  - YYYY is optional and can be any positive integer value. If omitted, YYYY defaults to the current year. If a one- or two-digit year is entered, the century portion of the date defaults to 19.
  - MM is the month (1-12)
  - DD is the day of the month (1 - 28, 29, 30, or 31, depending on the month)
2. The default time for a date that is selected from the calendar is always 00:00:00 (midnight). To specify a different time, enter the time that you want in 24-hour format: hh:mm:ss, where hh is the hour (0-23), and mm and ss are minutes and seconds (both 0-59)..

Note: Some APIs accept dates or timestamps. In these cases, the format is always **yyyy-mm-dd**  
**hh:mm:ss**.

### Select a Relative Date from Date Picker

---

Rather than specify an exact date, it is often more convenient to specify dates relative to either the current date (now) or some other date (the first Monday, for example). For example, to always include information from the previous seven days in a query, it's more convenient to define relative dates (for example, **start = now minus seven days** and **end = now**). The Relative Date Picker tool can be used to select a relative date for many types of tasks.

1. Click the Relative Date Picker next to any field where a relative date is allowed. The Relative Date Picker window opens.
2. Select Now, Start, or End from the list. Depending on your choice, the display changes to provide for additional selections.
3. From the middle list, select this, last, or previous, which is relative to the unit (day, week, month, or day of the week) that is selected in the next list) as follows:

- This is the current unit.
  - Last is the current unit minus one.
  - Previous is current unit minus two.
4. Select the day, week, month, or a specific day: Monday-Friday.
  5. Click Accept when you are done. The relative date is inserted into the field next to the Relative Date Picker button that you clicked.
  - 6.

## Enter a Relative Date Manually

---

To enter a relative date manually, follow one of the procedures. The keywords are not case-sensitive but each component must be separated from the next by one or more spaces.

There are three general formats you can use to enter a relative date:

- NOW plus or minus a specified number of minutes, hours, days, weeks, or months.
- The Start or End of the current, last or previous day, week, or month.
- The Past or Previous day of the week (Sunday, Monday, Tuesday, and so on.).

## Relative to NOW

---

1. Click in the field where you want to enter the relative date. Depending on the application, you can either search for data in the past (such as from a report) or schedule an action in the future (to start a service).
2. Enter the keyword NOW.
3. To search for existing data, enter a minus sign and an integer to specify the relative time. To specify a future action, specify a plus sign and an integer.
4. Specify one of the following keywords: HOUR, DAY, WEEK, or MONTH. Plurals (hours, days, etc.) are not allowed.

Examples:

- To query data from a report for the last 12 hours, enter NOW -12 HOUR.
- To start an S-TAP installation via GIM in exactly one day, enter NOW +1 DAY.

Note: Some APIs also accept relative dates. Enter the relative date as, for example, NOW +3 DAY or NOW -12 HOUR. For APIs, the text is case-sensitive.

## Relative to a Day, Week or Month

---

1. Click in the field where you want to enter the relative date.
2. Enter the keywords START OF or END OF.
3. Enter THIS or LAST, followed by DAY, WEEK, or MONTH. Example: end of last week

## Relative to a Day of the Week

---

1. Click in the field where you want to enter the relative date.
2. Enter the keywords START OF or END OF.
3. Enter LAST or PREVIOUS, followed by SUNDAY, MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, or SATURDAY. Example: start of previous Tuesday

## Building Time Periods

---

Policy rules and query conditions can test for events that occur (or not) during user-defined time periods.

When you open the Time Period Builder, a set of pre-defined time periods is available. You can edit the available time periods to meet your needs or you can define your own.

## Adding a time period

---

1. Browse to the Time Period Builder by clicking Setup > Tools and Views > Time Period Builder.
2. Click  to open the Add Time Period page.
3. You can create either contiguous or repeating block time period. For example, the following two custom time periods both begin at 09:00 (9 AM) Monday and end on 17:00 (5 PM) Friday:
  - Workweek is contiguous and defines a single 164-hour period beginning at 9 AM on Monday and ending at 5 PM on Friday.
  - Workday is a repeating block (that is, noncontiguous) and defines five separate eight-hour time periods (9 AM – 5 PM), on five consecutive days (Monday – Friday).
4. In the Name box, enter a name for this time period. For this example, enter either Workweek or Workday.  
Note: Do not use apostrophes (') in the description.
  - For Workweek, select Contiguous.
  - For Workday, select Repeating block.
5. Enter a beginning time in hours (00-24) and minutes (00-59) in the Hour From box. For this example, enter 09:00.
6. Enter an ending time in hours (00-24) and minutes (00-59) in the Hour To box. For this example, enter 17:00.
7. Select a beginning day of the week in Weekday From.
8. Select an ending day of the week in Weekday To.
9. Click OK to save the new time period.

Note: When you define a time period, Sunday is always assumed to be the first day of the week. Therefore, if you define a full week, you must start with Sunday. That is, you can set DAY FROM to Sunday and DAY TO to Saturday, but setting DAY FROM to Monday and DAY TO to Sunday returns unexpected results.

## Editing a Time Period

---

1. From the Time Period Builder, select an existing time period and click  to open the Edit time period page.
2. Change any fields as needed in the Edit time period page for the selected time period.
3. Click OK to save your changes.

## Removing a Time Period

---

From the Time Period Builder, select the time period that you want to remove, and click  to delete the selected time period.  
Note: You cannot delete a time period that is used by an existing policy rule.

---

## Cipher suites

---

Cipher suites are combinations of cryptographic parameters that define the security algorithms and key sizes.

Guardium® uses operating system level ciphers for many different purposes, such as,

- GIM agent
- SSH
- S-TAP agents (both Windows and Linux®)
- Guardium inspection core (that is, the Guardium sniffer)

Use the **show ssl\_configuration** CLI command to view the ciphers configured for the sniffer. For example,

```
my.example.com> show ssl_configuration
```

Sample output

```
TLS 1.2/ OpenSSL 1.x Ciphers
(1) [X] AES128-SHA
(2) [X] AES256-SHA
(3) [] AES256-SHA256

TLS 1.3/ OpenSSL 3.x Cipher Suites
(4) [X] TLS_AES_128_GCM_SHA256
(5) [X] TLS_AES_256_GCM_SHA384
(6) [X] TLS_CHACHA20_POLY1305_SHA256
(7) [] TLS_AES_128_CCM_SHA256
(8) [] TLS_AES_128_CCM_8_SHA256
```

ok

To change the SSL ciphers, use the **store ssl\_configuration** CLI command.

For more information, see the [store ssl\\_configuration](#) command in [Configuration and control CLI commands](#).

Note: If you run Linux or UNIX, use the **nmap -sV --script ssl-enum-ciphers -p <port\_number> <appliance>** command to list all of the ciphers available on the Guardium appliance.

For a list of the ports that Guardium uses, see [Guardium port requirements](#).

## Hashing user passwords

---

Guardium uses the following cipher to hash user passwords:

PBKDF2-SHA512 cipher

## GUI encryption ciphers

---

To view and manage the ciphers that are used between clients and servers in the Guardium GUI, use the **show ssl\_gui\_ciphers** CLI command. For example,

```
my.example.com> show ssl_gui_ciphers
1. SSL_ECDHE_RSA_WITH_AES_256_GCM_SHA384
2. SSL_ECDHE_RSA_WITH_AES_256_GCM_SHA256
3. SSL_ECDHE_RSA_WITH_AES_128_GCM_SHA384
4. SSL_ECDHE_RSA_WITH_AES_128_GCM_SHA256
5. SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
6. SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
7. SSL_ECDHE_RSA_WITH_AES_256_CBC_SHA384
8. SSL_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
9. SSL_ECDH_RSA_WITH_AES_256_CBC_SHA384
10. SSL_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
11. SSL_ECDHE_RSA_WITH_AES_256_CBC_SHA
12. SSL_ECDH_ECDSA_WITH_AES_256_CBC_SHA
13. SSL_ECDH_RSA_WITH_AES_256_CBC_SHA
14. SSL_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
15. SSL_ECDHE_RSA_WITH_AES_128_CBC_SHA256
16. SSL_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
17. SSL_ECDH_RSA_WITH_AES_128_CBC_SHA256
18. SSL_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
19. SSL_ECDHE_RSA_WITH_AES_128_CBC_SHA
20. SSL_ECDH_ECDSA_WITH_AES_128_CBC_SHA
```

21. **SSL\_ECDH\_RSA\_WITH\_AES\_128\_CBC\_SHA**  
ok

For more information about the **ssl\_gui\_ciphers** commands, see [delete ssl\\_gui\\_ciphers and restore ssl\\_gui\\_ciphers](#) in [Configuration and control CLI commands](#).

## File backup cipher

Guardium uses the following cipher to encrypt and decrypt files and backups:

- aes256

## MySQL encryption ciphers

MySQL encrypts data at rest by using AES\_ENCRYPT() and AES\_DECRYPT(), which are considered to be the most cryptographically secure encryption functions that are currently available in MySQL. SHA-2, DES, and AES functions require MySQL to be configured with SSL support.

## Related reference

- [Guardium port requirements](#)

## Comments

Comments apply to definitions and to workflow process results.

Comments can be added or viewed in several places throughout the UI. You can add a comment to a group or alias for reference purposes, or add a comment to report to ease auditing requirements. For example, an auditor may want to know why a configuration change was made on a certain date. Use a comment to easily reference the reason why the change was made.

Comments apply to definitions (groups, aliases, reports, policies), and to workflow process results. You can add multiple comments to a component, and you can add comments to comments, but you cannot modify or delete existing comments.

There are two different kinds of comments:

- **Comments Entities** are stored on the Central Manager, and will be available within that Central management environment, given the usual constraints regarding roles and permissions.
- **Local Comments Entities** are defined on a single unit, and remain local to that unit. Local Comments from the standalone or managed unit are not stored on the Central Manager.

## Add or View Comments

1. To view comments, open the User Comments window by clicking Comply > Reports > User Comments.
2. Throughout the UI, there are different ways to add a comment to an entity or report.
  - Add a comment to a group by modifying the group, and clicking Add Comments from the Manage Members for Selected Group screen.
  - Add a comment to an alias by opening the Alias Builder and clicking the Comment icon  . Open the Alias Builder by clicking Setup > Tools and Views > Alias Builder

## Report Comments

View a report of all user comments by clicking Comply > Reports > User Comments.

- The Local Comments entity is used in a Central Manager environment only. Local comments remain local to the system on which they were defined, and are not stored on the Central Manager.
- The Comments entity contains comments that are stored on the Central Manager.

## Customer Uploads

The Database Protection Subscription Service supports the maintenance of predefined assessment tests, SQL based tests, CVEs, APARs, and groups such as database versions and patches.

Uploads are used to keep information current and within industry best practices to protect against newly discovered vulnerabilities. Updates are distributed quarterly.

Use Customer Uploads to upload the following types of files: DPS update files; Oracle JDBC drivers; MS SQL Server JDBC drivers; and, DB2 for z/OS license jar files.

Note: If a custom group exists with the same name as a predefined Guardium® group, the upload process adds Guardium in front of the name for the predefined group.

1. Open Customer Uploads by clicking Harden > Vulnerability Assessment > Customer Uploads.
2. For DPS Upload, click Browse to locate and select the file to be uploaded.
  - a. Navigate to Harden > Vulnerability Assessment > Customer Uploads.
  - b. In the DPS Upload section, click Browse and choose the latest DPS update file, then click Upload.
  - c. In the Import DPS section, click  to import the DPS update.

Note: The DPS file can take a long time to install. If you restart the browser, the install stops. Either keep the Customer Upload window open until you see a status message, or use the CLI command `show dps` to check install status. Reference the Import DPS pane to see what files have been uploaded.

3. For Upload DB2 z/OS License jar, click Browse to locate and select the file.

4. Use Upload Oracle JDBC driver or Upload MS SQL Server JDBC driver to upload open source drivers. After the upload finishes, you will see the databases that are added to the Select datasource window. Upload one driver at a time.

Note: There are two instances where open source drivers are recommended over Oracle Data Direct drivers or MS SQL Data Direct drivers.

a. To support Windows Authentication for MS SQL Server. In all other uses, the Data Direct driver pre-loaded in the Guardium appliance is sufficient.

b. When you use the Value Change Tracking application for Oracle version 10 or higher, the open-source driver is recommended in order to support the use of streams instead of triggers.

Use keywords to search and download open source JDBC drivers (for example: *open source JDBC driver for MS SQL*).

5. Use the Central Manager to distribute the .jar file to managed units. After the file is successfully uploaded, the GUI needs to be restarted on the Central Manager and the managed units.

Note: If you will be exporting and importing definitions from one unit to another, be aware that subscribed groups are not exported. When you export definitions that reference subscribed groups, ensure that all referenced subscribed groups are installed on the importing unit (or central manager in a federated environment). When uploading DB2® z/OS® license jar files, the license will take effect after restart of the GUI.

Note: If the DPS stops for any reason (for example, a server restart or a GUI restart), it is recommended to wait 30 minutes before starting the DPS upload process again.

Enable ASO on the Oracle server using latest Oracle DataDirect driver

Refer to the following information when you enable ASO on the Oracle server that uses the latest Oracle DataDirect driver.

SQLNET.CRYPTO\_CHECKSUM\_SERVER = required

SQLNET.ENCRYPTION\_SERVER = required

SQLNET.ENCRYPTION\_TYPES\_SERVER = (AES256, AES192, AES128)

#SQLNET.CRYPTO\_CHECKSUM\_TYPES\_SERVER = (SHA256)

SQLNET.CRYPTO\_CHECKSUM\_TYPES\_SERVER = (SHA1)

The Oracle JDBC driver will work and does not require specifying a connection property. Download the latest Oracle JDBC driver that is compatible with your database version, then upload that driver to the system using the Guardium Customer Uploads function.

If you continue to use Oracle DataDirect driver, then you need to specify a connection property to the datasource.

Use the following when defining the Oracle DataDirect driver connection property:

DataIntegrityLevel=required;EncryptionLevel=required;DataIntegrityTypes=(MD5,SHA1)

Note: The current Oracle DataDirect driver does not support SHA-256. So SHA-1 has to be used. That is why sqlnet.ora reference (#SQLNET.CRYPTO\_CHECKSUM\_TYPES\_SERVER = (SHA256)) had to be commented out. However, if a Guardium customer must connect using SHA-256, they need to use the Oracle JDBC driver instead.

Data Direct references:

<https://www.progress.com/documentation/datadirect-connectors>

Download the Oracle database JDBC User' Guide PDF for a list of command references.

Use a tab-delimited file (.TXT) when creating and saving a Datasource Upload file from the Customer Upload functionality

If you choose to use a comma-delimited file structure (.CSV), it will not behave as intended if any column value contains a comma.

Follow these steps:

1. If using EXCEL, save file as a tab-delimited (.TXT) file.
2. If using OpenOffice or Libre Office then save a (.CSV) file with TAB Delimiters.
3. Log in as admin and open Customer Uploads by clicking Harden->Configuration Change Control (CAS Application)->Customer Uploads.
4. For Upload CSV to Create/Update Datasources, click Browse..., and select the tab-delimited file.

## Upload CSV file to create or update datasources

Follow the proceeding steps to create a tab-delimited .TXT formatted file containing datasource information. This tab-delimited .TXT file can then be used with the Customer Upload function in the Guardium application to many datasource types.

Use the function to import datasources was not always compatible with each Guardium Software Release. This procedure will enable the uploading of any datasource.

The following is a list of Header Columns that should be added to an Excel spreadsheet when creating the .TXT tab-delimited datasource upload file:

Column Values (accepted for .CSV datasource upload file)

Table 1. create\_datasource

| Parameter | Description |
|-----------|-------------|
|-----------|-------------|

| Parameter           | Description                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| application         | Required. Identifies the application for which the datasource is being defined. It must be one of the following:<br><br>ChangeAuditSystem<br>Access_policy<br>MonitorValues<br>DatabaseAnalyzer<br>AuditDatabase<br>CustomDomain<br>Classifier<br><br>AuditTask<br>SecurityAssessment<br>Replay<br>Stap_Verification                                                          |
| compatibilityMode   | Compatibility Mode: Choices are Default or MSSQL 2000. The processor is told what compatibility mode to use when monitoring a table.                                                                                                                                                                                                                                          |
| conProperty         | Optional. Use only if additional connection properties must be included on the JDBC URL to establish a JDBC connection with this datasource. The required format is property=value, where each property and value pair is separated from the next by a comma.<br><br>For a Sybase database with a default character set of Roman8, enter the following property: charSet=utf8 |
| customURL           | Optional. Connection string to the datasource; otherwise connection is made using host, port, instance, properties, etc. of the previously entered fields. As an example this is useful for creating Oracle Internet Directory (OID) connections.                                                                                                                             |
| dbInstanceAccount   | Optional. Database Account Login Name (software owner) that will be used by CAS                                                                                                                                                                                                                                                                                               |
| dbInstanceDirectory | Optional. Directory where database software was installed that will be used by CAS                                                                                                                                                                                                                                                                                            |
| dbName              | Optional. For a DB2 or Oracle datasource, enter the schema name. For others, enter the database name.                                                                                                                                                                                                                                                                         |
| description         | Optional. Longer description of the datasource.                                                                                                                                                                                                                                                                                                                               |
| host                | Required. Can be the host name or the IP address.                                                                                                                                                                                                                                                                                                                             |
| name                | Required. Provides a unique name for the datasource on the system.                                                                                                                                                                                                                                                                                                            |
| owner               | Required. Identifies the Guardium user account that owns the datasource.                                                                                                                                                                                                                                                                                                      |
| password            | Optional. Password for owner. If used, user must also be used.                                                                                                                                                                                                                                                                                                                |
| port                | Optional (integer). Port number.                                                                                                                                                                                                                                                                                                                                              |
| serviceName         | Required for Oracle, Informix®, DB2, and IBM® iSeries. For a DB2 datasource, enter the database name. For others, enter the service name.                                                                                                                                                                                                                                     |
| severity            | Optional. Severity Classification (or impact level) for the datasource.                                                                                                                                                                                                                                                                                                       |
| shared              | Optional (boolean). Set to <b>true</b> to share with other applications. To share the datasource with other users, you will have to assign roles from the GUI.                                                                                                                                                                                                                |
| type                | Required. Identifies the datasource type. For a list of supported datasource types, use the <code>list_db_drivers</code> API command:<br><br><code>grdapi list_db_drivers</code><br><br>For more information, see <a href="#">list_db_drivers</a> .                                                                                                                           |
| user                | Optional. User for the datasource. If used, password must also be used.                                                                                                                                                                                                                                                                                                       |
| role                | Optional. One or more user roles that can access the datasource. Separate roles by using a semicolon.                                                                                                                                                                                                                                                                         |
| environmentTitle    | Required for cloud database service protection. Account name.                                                                                                                                                                                                                                                                                                                 |
| region              | Required for cloud database service protection. The AWS region.                                                                                                                                                                                                                                                                                                               |
| objectLimit         | Required for cloud database service protection with native audit. The maximum number of objects found in the classification process that are added automatically to the list of audited objects. See <a href="#">Cloud database service protection</a> .                                                                                                                      |
| primaryCollector    | Relevant for cloud database service protection. The collector that extracts the audit data from the cloud database.                                                                                                                                                                                                                                                           |

Notes:

1. Each of the column names must be included in the Excel spreadsheet SAVED as a tab-delimited (.TXT) file.
2. The Created Datasource name (what is shown when looking for the datasource) is made up of both the name column and the type column.
3. Upload file MUST be saved as a Column Tab Delimited file type.

Steps to create and upload txt file in a Text CSV format file and add Datasource Data

1. Create the Excel spreadsheet file save as a tab-delimited .TXT file with the following headers and datasource data to support the datasource import capability.
2. Create and save your .txt file to your PC or UNIX/Linux device for uploading into the Guardium application.
3. Log in as admin and open Customer Uploads by clicking Harden > Configuration Change Control (CAS Application) > Customer Uploads
4. From Upload CSV to Create/Update Datasources, click Browse and select the .txt file containing the tab-delimited datasource information.
5. Click Upload.

A message displays showing which values from the .txt file were uploaded:

1. **New:** Per file upload (if save file and added New Datasource member(s), these members returns the status of NEW.
2. **Update:** Uploading the same datasource on which you made changes returns an Update status.
3. **Fail:** Displayed failed datasource or errors

# Stream Guardium data to another application

Use the Data Streaming to send traffic collected by Guardium to another tool for analysis.

## About this task

### Procedure

1. Open the Data Streaming configuration page.
  - To configure a standalone system or a single managed unit in an environment with a central manager, navigate to **Setup > Tools and Views > Data Streaming**.
  - To configure multiple managed units from a central manager, navigate to **Manage > Central Management > Distribute Configuration Profiles** and work with a configuration profile where the Configuration type is Data streaming configuration. For more information about configuration profiles, see [Working with configuration profiles](#).
2. Use the Stream to menu to select a destination for Guardium Data Activity Monitoring traffic.
  - IBM Security Guardium is the default behavior: Guardium data is stored locally.
  - IBM Security Guardium Big Data Intelligence sends traffic to Guardium Big Data Intelligence. Data is not stored locally.
  - Datamart for Guardium Insights stores data locally and periodically syncs with IBM Security Guardium Insights.  
Note: Selecting this setting sends traffic to Guardium Insights. Verify that Guardium Insights is configured to receive and analyze traffic from the Guardium system.
3. Click Save to save the configuration.  
On a standalone system or a single managed unit, the selected settings are immediately enabled. On a central manager, complete the configuration profile and distribute the settings to managed units.

## Big Data Intelligence

The Guardium Big Data Intelligence (GBDI) platform stores collected data over longer timeframes, providing direct, near real-time access to data security and compliance reports and insights.

Note: If your site uses GBDI with data marts, you can reconfigure your site to use data streaming.  
You can provide access to Guardium Big Data Intelligence (GBDI) in two different ways:

- [Big Data Intelligence with data marts](#)  
Guardium® Big Data Intelligence uses data marts to export data to a central storage location.
- [Big Data Intelligence with data streaming](#)  
Use data streaming to Guardium Big Data Intelligence (GBDI) to stream audit data directly from your Guardium system to the GBDI platform.

### Related concepts

- [Domains, Entities, and Attributes](#)

## Big Data Intelligence with data marts

Guardium® Big Data Intelligence uses data marts to export data to a central storage location.

To deploy and use Guardium Big Data Intelligence:

1. Define the central storage. Use the GuardAPI **create\_datasource** or the GUI ([Creating a datasource definition](#)). Use Big Data Intelligence as the application type.
2. Define your data export profile by using the GuardAPI Big Data Intelligence function **enable\_big\_data\_interface**. The profile defines the datasource, the target host, the units that export data, the data mart extraction profile (made up of one or more data marts), and the export schedule. There are four predefined, non-modifiable profiles. To create your own data export profile, copy and modify the predefined profiles. You must use the data marts specified in the predefined profiles in order to access your data in the Big Data Intelligence domains of the Query-Report Builder.  
The profile is applied to the managed units you specify in the command **enable\_big\_data\_interface**; all the managed units of the central manager, and to the central manager itself, a managed unit group, or specific managed units.
3. After you run **enable\_big\_data\_interface** you'll see Big Data Intelligence domains in the Query-Report Builder. When you define a query, Guardium needs to connect to the GBDI to validate and save the query. This can take up to a minute. Watch the lower left corner of your GUI; you'll see text waiting for server until it connects. If Guardium cannot connect to the GBDI, it responds: *Unable to establish connection...*, and the query is not saved.
4. Use the standard Guardium predefined reports and Investigation Dashboards (Quick Search) to analyze your data. You can also create reports using the Big Data Intelligence domains.

You can enable additional managed units for data extraction at a later date with the command **grdap local\_enable\_big\_data\_interface profile\_name="<profile name>"**. This is useful if a collector was offline or not in the MU group when the interface was enabled; or, for advanced users, if you want to include data from a collector that requires a different profile, or is in another group. For example, two managed units of a central manager run only VA, and the other managed units are tracking other data. You would create a second profile that is a subset of the main profile, and run it only on the specified units. However, the local profile does not have a target for the data; add it using the command: **datamart\_update\_copy\_file\_info**.

## Data handling guidelines

- Data retention on the collector can be reduced to 1 day since the Big Data Intelligence server saves data over a long time period.
- Data backup can be handled on the Big Data Intelligence server.
- Configuration backup should be handled on the Guardium system.

- Archives should be handled according to your regulation requirements. The Big Data Intelligence server keeps data longer than collectors and aggregators, and can be used for archiving.

The Guardium capabilities to read Big Data Intelligence directly using the Guardium Query-Report Builder, or enterprise search, require Guardium Big Data Intelligence Version 3.3. If you already have a data mart extraction to an earlier GBDI version, disable the extractions that are running, and then re-enable by using the following API: **enable\_big\_data\_interface**

## Summary of data marts in each profile

---

### Basic summary

Export:Access Log, Export:Session Log, Export:Session Log Ended, Export:Exception Log, Export:Full SQL, Export:Outliers List - enhanced, Export:Outliers Summary by hour - enhanced, Export:Group Members, Export:Export Extraction Log, Export:Policy Violations, Export:Buff Usage Monitor

### Comprehensive summary

Export:Access Log, Export:Session Log, Export:Session Log Ended, Export:Exception Log, Export:Full SQL, Export:Outliers List - enhanced, Export:Outliers Summary by hour - enhanced, Export:Group Members, Export:Export Extraction Log, Export:Policy Violations, Export:Buff Usage Monitor, Export:VA Results, Export:STAP Status, Export:Discovered Instances, Export:Databases Discovered, Export:Classifier Results, Export:Installed Patches, Export:System Info

### Basic Details

Export:Access Log - Detailed, Export:Session Log, Export:Session Log Ended, Export:Exception Log, Export:Full SQL, Export:Outliers List - enhanced, Export:Outliers Summary by hour - enhanced, Export:Group Members, Export:Export Extraction Log, Export:Policy Violations - Detailed, Export:Buff Usage Monitor

### Comprehensive details

Export:Access Log - Detailed, Export:Session Log, Export:Session Log Ended, Export:Exception Log, Export:Full SQL, Export:Outliers List - enhanced, Export:Outliers Summary by hour - enhanced, Export:Group Members, Export:Export Extraction Log, Export:Policy Violations - Detailed, Export:Buff Usage Monitor, Export:VA Results, Export:STAP Status, Export:Discovered Instances, Export:Databases Discovered, Export:Classifier Results, Export:Installed Patches, Export:System Info

- [Configure key pair authentication for GBDI file extraction](#)

By default, Guardium uses a password for GBDI file extraction. Use this procedure to configure a key pair authentication instead of a password. You upload the file to the central manager, and from there distribute it to the relevant managed units.

## Related concepts

---

- [Data Mart](#)
- [Enterprise search](#)
- [Domains, Entities, and Attributes](#)

## Related reference

---

- [Big Data Intelligence APIs](#)

## Configure key pair authentication for GBDI file extraction

---

By default, Guardium® uses a password for GBDI file extraction. Use this procedure to configure a key pair authentication instead of a password. You upload the file to the central manager, and from there distribute it to the relevant managed units.

## About this task

---

Upload the key file to the central manager if you want to distribute it to managed units. You can upload it to an individual managed unit, but cannot distribute it from there to other managed units. When you upload the file to the Guardium system, it is deleted from the file server.

## Procedure

---

1. Upload the key to the file server.
2. On the central manager, upload the key file to all managed units with the GuardAPI command **copy\_key\_file**, for example:

```
grdapi copy_key_file fileName="/opt/IBM/Guardium/log/key-file" all="true"
```

The central manager copies (by SCP) the key file to all managed units, copies the file to the central manager, and deletes it from the file server. At the end it returns a list of all managed units with the status of the grdapi execution for each. If a unit is down, its status is failed.

3. For GBDI using data marts: Update the copy\_file details with the GuardAPI command **datamart\_update\_copy\_file\_info**, for example:

```
grdapi datamart_update_copy_file_info destinationHost=<server name> destinationPassword="file:key-file" destinationPath=<path> destinationUser=<user> Name="<datamart name>" transferMethod="SCP"
```

4. If distribution to a managed unit failed, upload the key to the file server on this unit and run the GuardAPI command **copy\_key\_file** on that unit.

```
grdapi copy_key_file fileName="<keyFile.key>"
```

5. To install a new key file, repeat steps 1, 2, and 3.

## Results

---

The key file is used for file transfer, instead of a password.

## Big Data Intelligence with data streaming

---

Use data streaming to Guardium Big Data Intelligence (GBDI) to stream audit data directly from your Guardium system to the GBDI platform.

With GBDI data streaming, monitored event data from your site is sent to Guardium collectors. From there, it is processed by the Guardium collector and the selected audit data is formatted into JSON documents and streamed to the security data lake on the GBDI platform. From the GBDI platform, you can use GBDI reporting and analytic tools.

When you enable GBDI data streaming, the Guardium collector generates JSON documents for the events you choose to monitor and log. The JSON documents are sent to GBDI for storage and analysis. In addition, other information is stored in a MySQL database on the Guardium database server.

The following information can be collected and streamed to GBDI:

- Session: Contains details about the event session such as DB name, client and server ports, session start, and end, server type, client IP, and other information.
- Instance: For each SQL statement, the streamed data includes the ConstructID, original SQL statement, any objects and verbs included in that statement, and other objects.  
Note: For Instances, the difference between MySQL and data streaming is as follows:
  - For MySQL, detailed SQL construct information is logged in separate GDM tables: GDM\_CONSTRUCT, GDM\_SENTENCE, and GDM\_OBJECT.
  - With data streaming, construct information is part of the instance document, including original\_sql, objects and verbs.
- Full\_SQL: Includes all of the relative information relative to the event. This information includes data (masked or unmasked, depending on the policy rule action), the returned data count, and the total number of records affected.
- Policy\_violations: Includes any policy violation information. Each policy violation message has a unique identifier, which is referenced in the Guardium alert when the alert template variable %ViolationID is configured.
- Exception: Collects sniffer exceptions and errors. Depending on the policy rule action, the SQL string can be either full or masked.
- [Configure GBDI data streaming](#)  
To configure and use Guardium Big Data Intelligence (GBDI) data streaming, install a jProxy connector to initiate and maintain the connection between the Guardium collector and the GBDI platform.

## Configure GBDI data streaming

To configure and use Guardium Big Data Intelligence (GBDI) data streaming, install a jProxy connector to initiate and maintain the connection between the Guardium collector and the GBDI platform.

### About this task

The jProxy connector is available as an RPM package within the Guardium installation package. After jProxy is installed, the Guardium collector sniffer component communicates with jProxy (rather than directly with GBDI).

The jProxy installation includes the following services:

- **sonarjproxyd**: A light-weight MongoDB server with some customized functionality for GBDI.
- **jproxytimer**: Controls service timing configuration, including starting jProxy and managing the intervals for flushing the data.

jProxy includes the following configuration files:

- **jproxy.conf**: sonarjproxyd service settings
- **jproxyforwarder.env**: jproxyforwarder service settings
- **logging.conf** : Log file and log level settings

Use the CLI commands, described in the Procedure section, to update the configuration file settings.

Note: Every CLI **store** command that is described in this section has a matching **show** command that displays the current stored value.

### Procedure

1. From your Guardium collector, call the following CLI command to control the sniffer logger destination.

```
store snif_logger_destination_type [LOCAL | REMOTE]
```

Where:

- LOCAL (default) sets the logger destination to the local database on the Guardium collector.
- REMOTE sets the logger destination to the intermediate database used by GBDI.

2. For security reasons, each GBDI machine provides an authentication key file (SSH key) to secure data communication between the Guardium collector and GBDI.

Use the following CLI commands to upload the GBDI SSH key file (in .pem format) and configure the SSH target host to communicate with GBDI:

- **import jproxy\_files**
- **store jproxy\_config ssh\_key\_file <key\_file\_name>**

Take the following steps to import and store the SSH key file:

- a. Call **import jproxy\_files** to import the jProxy ssh key file from the specified location.
- b. Call **store jproxy\_config ssh\_key\_file <key\_file\_name>** to store the key file in the key store.

3. Then, use the following CLI commands to configure information such as logger destination, Mongo client authentication (username, auth, database, and mechanism).

Note: All of the following configuration commands are optional. You can use these commands to change the defaults, if needed.

- **store logger\_data\_destination\_config type <database type>**  
The default value = "mongodb"
- **store logger\_data\_destination\_config database\_name <db name>**  
The default value = "sonargd"
- **store logger\_data\_destination\_config destination [hostname | port] <value>**
  - The default value for hostname = "localhost"

- The default value for port = "27118"
  - `store logger_data_destination_config [auth_username | auth_database_name | mechanism] <value>`
    - The default value for auth\_username = "enchantedsdg"
    - The default value for auth\_database\_name = "admin"
    - The default value for mechanism = "plain"
4. Optionally, use the following CLI command to specify the collections that you want to stream. The default for all collections is ON.
- ```
store logger_data_destination_config data <collection_type> [on|off]
```

The collection types are:

- session
- instance
- full_sql
- policy_violations
- exception

5. Optionally, use the following CLI commands to configure the streaming interval for transporting the JSON document data from Guardium to GBDI. Whenever Guardium hits either threshold, jProxy sends the data to GBDI.

- `store jproxy_config flush_timeout_sec <seconds>`
The default is 60 seconds.
- `store jproxy_config flush_at_size <bytes>`
The default is 102400000

What to do next

After you set the `store snif_logger_destination_type` to REMOTE and store the jProxy SSH key, the data collections are automatically streamed to the GBDI platform. From there, you can use the GBDI data analytic tools as needed.

In addition, data is also stored in the Guardium MySQL database.

Exporting and importing definitions

Use export and import definitions if you have multiple systems with identical or similar requirements and are not using central management. You can define the components that you need on one system and export those definitions to other systems that are on the same software release level.

You can export one type of definition (reports, for example) at a time. Each element that you export can cause other referenced definitions to be exported as well. For example, a report is always based on a query, and it can also reference other items, such as IP address groups or time periods. All referenced definitions (except for security roles) are exported along with the report definition. However, only one copy of a definition is exported if that definition is referenced in multiple exported items. An export of policies or queries exports only the groups that are referenced by the exported policies or queries.

Using export and import definitions

Use Definitions export and Definitions import to save and then restore functional data from a specific Guardium system. For example, you can create a report on one Guardium system and then import that same report onto another server (of the same Guardium installed version).

Note: The export and import function is not the same as a full backup of the server. Be sure that you still define and run backups on a scheduled or manual basis.

UseDefinitions export to save and share defined functional values such as reports and queries, CAS data, or classifier data. The export types are saved as .sql files.

You can import the exported definitions onto servers that use the same Guardium Software version. In general, if you export definitions from a Guardium V10 system, then you can import those definitions only onto another V10 system.

You can export data marts and reports from an earlier version and import to a later version. For example, you can export definitions from a Guardium V10 system and import the definitions onto a V11 system. However, you cannot export from a later version to an earlier version.

Export definitions rules

When you export definitions, Guardium cannot export the following elements:

- For graphical reports, the presentation parameter settings (such as colors, fonts, or titles) are not exported. When imported, these reports use the default presentation parameter settings for the importing system.
- Subscribed groups are not exported. When you export definitions that reference subscribed groups, make sure that all referenced subscribed groups are installed on the importing appliance (or the central manager in a centrally managed environment).
- Comments are not exported.
- When you export a data source with an open source driver, the open source driver is not included in the export. Upload the open source driver into the new system before you import the data source definition that was created by using it. If the open source driver is not available during the import, Guardium substitutes the data direct driver.
- When you export the definition of classifier policies, any custom evaluation classes that are associated with the policies are not exported with the definition. For the imported policies to work, upload the custom evaluation classes separately.

In addition, be aware of the following rules before you export definitions.

- You cannot import or export definitions between different languages. For example, if you export a file from a Simplified Chinese Guardium® system, you cannot import the file to a system where the language is set to English.
- Definitions export and import logs have the same retention period as the monitored database activity logs.
- When you export audit process definitions of scheduled runs (including schedule time) to another system, the Active checkbox in Audit Process Builder is never checked.
- For Schedule start time of an audit process that is defined on one appliance and exported to another (unrelated) appliance; if the original schedule start time is defined, it is retained. If the original schedule start time is not defined (empty), then the imported schedule start time is set to the time it was imported.

- Large complex imports can take a long time and can exceed the length of the user's session. If the session times out, the import continues to run in the background until it completes.

Import definitions rules

Before you import definitions, make sure you understand the following rules.

- When you import an existing group, members can be added, but members are not deleted.
- When you import aliases, new aliases can be added, but aliases are not deleted.
- When a definition is created, the user who creates it is saved as the owner of that definition. Therefore, if no security roles are assigned to that definition, only the owner and the admin user have access to it.
- When you import a definition, the owner is always changed to admin.
- References to security roles are removed from exported definitions. Therefore, any imported definitions do not have assigned roles.
- A reference to a user in an exported definition causes the user definition to be exported. When definitions are imported, the referenced user definitions are imported only if they do not exist on the importing system. In other words, existing user definitions are never overwritten. The implications are described in [Duplicate Group and User Implications](#).

In addition, imported user definitions are disabled. Imported users can receive email notifications that are sent from the importing system, but they cannot log in to that system, unless and until the administrator enables that account.

Duplicate Group and User Implications

If a group that is referenced by an exported definition exists on the importing system, the definition of the exported group is not imported. If the group is not used for the same purposes on both systems, this might create some confusion.

If a user definition exists on the importing system, it might not be for the same person that is defined on the exporting system. For example, assume that on the exporting system the user jdoe with the email address john_doe@example.com is a recipient of output from an exported alert. Assume also that on the importing system, the jdoe user exists for a person with the email address jane_doe@sample.com. The exported user definition is not imported, and when the imported alert is triggered, email is sent to jdoe at jane_doe@sample.com. In either case, when security roles or user definitions are not imported, check the definitions on both systems to see whether differences exist. If so, make the appropriate adjustments to those definitions.

Definition Types for Exporting

Table 1. Definition Types for Exporting

Can export	Cannot export
Alert	Custom Alerting Class For alerts, you can choose to exclude group members. For more information, see the description under Group .
Alias	Custom Assessment Test
Audit process	Custom Identification Procedure
Auto-discovery process	
AWS Secrets Manager configuration	
CAS hosts	
CAS template Sets	
Classification process	Access Rule
Classifier policy	
Cloud service account	
Compound attribute	
Configuration profile	
Custom class connection permission	
Custom domain	
Custom table	
CyberArk configuration	
Dashboard	
Data classifier	
Datamart	
Datasource	
Datasource custom field	
Datasource group	
Discover sensitive data	
Distributed reports	

Can export	Cannot export
Event type	
External feed	
External ticket configuration	
Group	The Exclude group members option displays for data sets that have groups somewhere in the export hierarchy (for example, exporting an alert includes the alert query, and the query might include groups in the query conditions). If the export does not include groups, the Exclude group members option does not display. When the option is set, the export file includes groups (if groups are linked to the exported definition) but members of the groups are not exported. The option is not set by default. In addition, the state is not persistent and it applies only to the current export.
HashiCorp configuration	
IMS definition	
Investigation dashboard	
Kerberos configuration	
LDAP user import config	Passwords
Named template	
Period (time period)	
Policy (but not an included baseline)	
Privacy set	
Query	
Query rewrite definition	
Replay	
Report	For reports, you can choose to exclude group members. For more information, see the description under Group .
Role	
Security assessment	
Security assessment with no datasources	For security assessments with no datasources, you can choose to exclude group members. For more information, see the description under Group .
User	
Users database mapping	
Users database permission	
Users hierarchy	

Exporting definitions

1. Go to [Manage > Data Management > Definitions Export](#). The Definitions Export page opens.
2. Select an option from the Type menu. The Definitions to Export menu populates with definitions of the selected type.
3. Select all of the definitions of this type to be exported.
4. Click Export. Depending on your browser security settings, you might receive a warning message that asks if you want to save the file or to open it using an editor.
5. Save the exported file in an appropriate location.

Importing definitions

1. Go to [Manage > Data Management > Definitions Import](#). The Definitions Import page opens.
2. Click Browse to locate and select the file.
3. Click Upload. You are notified when the operation completes and the definitions that are contained in the file are displayed. Repeat to upload additional files.
4. Use the Fully synchronize group members checkbox to set the behavior of how to add new group members imported directly or via other data sets such as queries or policies. If not checked, new members that are in the import are added, but members not in the import are not removed. If checked, then group members not in the import are removed. Use the Set as default button next to the checkbox to save the checkbox setting.
5. Click Import this set of Definitions to import a set of definitions, or click Remove this set of Definitions without Importing to remove the uploaded file without importing the definitions.
6. You are prompted to confirm either action.
Note: An import operation does not overwrite an existing definition. If you attempt to import a definition with the same name as an existing definition, you are notified that the item was not replaced. If you want to overwrite an existing definition with an imported one, you must delete the existing definition before performing the import operation.

Exporting to XACML Protocol

Guardium supports export of Policy Rules to a XACML file, and import of XACML files to another Guardium system.

The XACML (eXtensible Access Control Markup Language) is a declarative access control policy language that is implemented in XML and a processing model, describing how to interpret the policies.

Note: XACML imports from previous versions of Guardium are not supported.
To export Guardium policies to XACML, follow these steps:

1. Click **Manage > Data Management > Export**.
2. Select **Policy** from the Type menu.
3. Check the **Export to XACML File** check box.
4. Select **definitions** from the Definitions to Export menu.
5. Click **Export**.

To Import an XACML file from another Guardium system, open the Definitions Import by clicking **Manage > Data Management > Import**.

Remote loggers

View the forwarding rules for the remote logging and test the connections.

Guardium sends system and other messages to syslog. Remote logging allows Guardium to send system and other messages to a remote receiver (such as an SIEM) by using the [store remotelog add](#) CLI.

After you configure remote logging, use the Remote loggers page to view and test the connectivity for existing remote logs.

To open the Remote loggers page, browse to **Setup > Tools and Views > Remote Loggers**. The remote logs that are configured for your current machine display.

- To download a list of all logs as a CSV file, click the  icon.
- To test the connectivity of a log, select the log and click **Test Remote Logger**. Wait a moment for the response.
Note: Guardium cannot verify the response for loggers that are configured as UDP.

In addition, you can use the [export config](#) API command to propagate the configuration from a central manager to its managed units.

Related information

- [export config](#)
- [show remotelog](#)
- [store remotelog add](#)

Manage Custom Classes

Upload and maintain custom classes used in alerts or evaluations. Manage custom classes by clicking **Setup > Custom Classes**.

After you compile a class, it must be uploaded to the Guardium® system.

Uploading a Custom Class

1. You can upload a custom class for alerts or evaluations. Upload a custom class by clicking **Setup > Custom Classes**, then either **Alerts > Upload** or **Evaluations > Upload**
2. Enter a description for the custom class.
3. Click **Browse** to locate and select the class file that you want to upload.
4. Click **Apply**.

Updating a Custom Class

1. Select **Setup > Custom Classes**, then either **Alerts > Update** or **Evaluations > Update**.
2. Select the description of the class to be updated.
3. Click **Browse** to locate and select the class file that is to be used for the update.
4. Click **Apply**.

Deleting a Custom Class

1. Select **Setup**, then either **Alerts > Delete** or **Evaluations > Delete**
2. Select the description of the class to be deleted.
Note: You cannot remove a class that is in use by some other component (the installed policy, for example).
3. Click **Delete**.

GDPR readiness: Considerations when configuring Guardium

Learn how Personal Identification Information (PII) data gets stored on your Guardium system, and how to manage this.

Policy Builder

If Log full details is selected in your Policy Rule Actions in the Policy Builder, Guardium logs data for each separate request, with unmasked values. Depending on the type of traffic being examined, it could contain PII. For more information, see: [Rule actions](#)

Inspection Engine

If Inspect return data is selected in the Inspection Engine configuration, data from the traffic, including result sets, is returned to the Guardium collector. Depending on the type of traffic being examined, it could contain PII. For more information, see: [Network mirroring methods \(SPAN, N-TAP\) and related inspection engines](#)

Follow these deployment guidelines for GDPR readiness:

Encryption

If you need to configure Policy Rule Actions to *Log full details* or Inspection Engines to *Inspect Return Data*, consider encrypting the disks in the appliances. For more information, see: [How to partition with an encrypted LVM](#).

Purge Intervals

Guardium may capture debug information that could contain PII if the database traffic that triggered the exception contained PII. Guardium admins can purge data by setting the purge interval via the GUI purge panel or the CLI command **store purge objects age**. For more information, see: [Enabling and disabling the Investigation Dashboard](#).

The default for several of these items can be viewed using the CLI complementary command, [show purge objects age](#). Interval is defined as *number of days*.

SQL Masking

Guardium may capture PII if a SQL query that contains PII fails. For more information, see [Logging Exceptions](#).

Groups

Using groups makes it easy to create and manage classifier, policy and query definitions, as well as roll out updates to your S-TAP's and GIM clients. Rather than having to repeatedly define a group of data objects for an access policy, put the objects into a group to easily manage them.

- [Groups overview](#)

Group similar data objects together and use them in creating query, policy, and classification definitions. Use one of the many predefined groups, or create your own group by using the Group Builder.

- [Using the group builder](#)

The group builder provides at-a-glance information about group membership and use and several convenient methods for populating groups.

- [Using groups in queries and policies](#)

Short overview of conditional operators for queries and where to use groups in policies.

- [Example: Using groups to create rules and policies](#)

Use groups to quickly specify rule conditions in a policy.

- [Predefined Groups](#)

This section details the predefined groups in Guardium®.

Groups overview

Group similar data objects together and use them in creating query, policy, and classification definitions. Use one of the many predefined groups, or create your own group by using the Group Builder.

Groups are practical to use in many places. By grouping similar data objects, you can use the whole set of objects in policies, classifications, queries, and reports, rather than having to select multiple data objects individually.

If you need to change a query or policy, rather than applying those changes to each individual object, you can apply those changes to the group.

S-TAPs and GIM also use groups to make it easier to roll out updates across managed servers.

Group Builder

Use the Group Builder to create a new group or modify an existing group from the user interface.

To open the Group Builder, click **Setup > Group Builder**.

Use the Group Filter screen to sort through groups based on application type, group type, description, or category.

Types of groups

The field Group Type refers to the type of data that can be grouped. For example, *Server IP* expects data that is formatted as an IP address and *Users* expects to see names of users on the application.

Note: The contents of group type Managed Units are not validated as being Guardium managed units, and the group type is not used by internal Guardium applications such as enterprise load balancing.

Tuple groups

A tuple group allows multiple attributes to be combined together to form a single composite group member. Tuples can help simplify specifying conditions for reporting and policy rules. Three of an ordered set of values are called 3-tuple. An n-tuple is one with an n-set of value attributes.

Examples of tuple groups include:

- Tuple groups - Object/Command, Object/Field, Client IP/DB User, Server IP/DB User
- 3-tuple groups - Client IP/Source Program/DB User, DB User/Object/Privilege
- 5-tuple group - Client IP/Source Program/DB User/Server IP/Service Instance
- 7-tuple group - Client IP/Src App/DB User/Server IP/Svc. Name/OS User/DB Name

Use a slash (/) to separate values within a tuple. You can specify multiple tuple elements by using a wildcard (%).

Note: In a tuple query, if your data contains a backslash (\), and you specify LIKE GROUP, the result might be wrong. If the data includes a backslash, use IN GROUP instead.

Predefined groups

Guardium includes a number of predefined groups. Use the Group Filter and Group Type menu to browse the list of groups and find the one that best suits your needs.

Group types *DB User* and *DB Password* are by default only available to admin users. Modify the group roles if you want to change this default setting.

Overlapping group memberships

Groups members can be in more than one group.

For example, two predefined groups, *Create Commands* and *DDL Commands*, both have members that are named CREATE TABLE. If you query for either of these groups, all of the CREATE TABLE members from the reporting period are counted in that group.

In some cases, you might want to define a set of groups so that each member belongs to only one group. For example, suppose that for reporting purposes you need to group database users into 1 of two groups: employees or consultants. You can define each of those groups with the same subgroup type (Employee-Status, for example). When subgroups are used, you cannot add a member to a subgroup if that member was already added to another group with the same subgroup type.

Wildcards in members

Group members can include wildcard (%) characters for when the group is used in a query condition or policy rule.

Table 1. Wildcards in members

Member	Matches	Does not match
aaa%	aaa, aaazzz	zzzaaa, aaz
%bbb	bbb, zzzbb	bb, bbbzzz
%ccc%	ccc, ccczz, zzzcccc	cc, zzzcczz

Wildcards for security assessment test exceptions

To create a wildcard search within groups for security assessment test exceptions, preface the member name with (R). You can then create a regular expression search for the group by using period (.) and asterisk (*) operators to match exactly one character (.) or zero or more characters (*).

Note: Search parameters are case-sensitive.

Table 2. Wildcards for security assessment test exceptions

Member	Matches	Does not match
(R)aaa	aaa, zzaaa, aaazz	Aaa, zzaba
(R)aaa*	aaa, aaazzz	zzzaaa, aaz, AAA
(R)*bbb	bbb, zzzbb	bb, bbbzzz, Bbb
(R)*c.c*	cbc, ccc, _c3c123	cc, _CAC123

Managed Unit Groups

Managed unit groups and the groups that are created through the group builder that used for grouping elements are distinct. Groups that are created through the group builder help simplify creating and managing policies and clarifying the presentation of reports. For more information about managed unit groups, see [Creating managed unit groups](#).

Using the group builder

The group builder provides at-a-glance information about group membership and use and several convenient methods for populating groups.

Use the group builder to create and populate groups from a variety of sources including CSV files, external datasources, and existing groupd. In addition, the builder provides at-a-glance information about group membership and where groups are used in security policies, classifier policies, queries, and reports.

The group builder is accessible at Setup > Tools and Views > Group Builder.

- [Creating and editing groups](#)
Learn how to create and edit groups.
- [Viewing group membership and where groups are used](#)
Learn how to view group membership and identify the policies, reports, and queries where groups are used.
- [Populating groups](#)
The group builder supports several methods of adding members to groups.

Creating and editing groups

Learn how to create and edit groups.

Creating a group

Procedure

1. Open the group builder by navigating to Setup > Tools and Views > Group Builder.
2. Click the  icon on the Group Builder table.
3. Use the Create new group dialog to define a new group.
Provide a group description and use the Application type and Group type menus to define the group.
4. After defining the new group, use the Members tab to populate the group.
For information about populating groups, see [Populating groups](#).
5. Click Save to create finish defining the new group.

Editing a group

Procedure

1. Open the group builder by navigating to Setup > Tools and Views > Group Builder.
2. Select a group from the Group Builder table and click the  icon.
3. Use the Edit group dialog to modify group settings.
To add members to the group or modify group membership, use the Members tab. For information about populating groups, see [Populating groups](#).
4. Click Save to finish editing the group.

Viewing group membership and where groups are used

Learn how to view group membership and identify the policies, reports, and queries where groups are used.

Viewing group membership

About this task

The Members and Populated by columns of the Group Builder table summarize how many members are in a group and how the group is populated. The following procedure describes how retrieve detailed information about group membership and the methods used for populating the group.

Procedure

1. Open the group builder by navigating to Setup > Tools and Views > Group Builder.
2. Open the Edit group dialog by selecting a group from the Group Builder table and clicking the  icon.
3. View group membership on the Edit group dialog by clicking the Members tab.

Identify where a group is used

About this task

The Used in classifier, Used in policy, and Used inquiry columns of the Group Builder table provide an overview of where groups are used in Guardium. The following procedure describes how retrieve detailed information about the policies, queries, and reports where a group is used.

Procedure

1. Open the group builder by navigating to Setup > Tools and Views > Group Builder.
2. Open the details panel by selecting a group from the Group Builder table and clicking Actions > View details.
Attention: The View details action is only enabled when the selected group is being used, for example by policies or queries.
3. Use the Policies and Queries tabs on the details panel to view where the selected group is used in security policies, classifier policies, queries, and reports.

Populating groups

The group builder supports several methods of adding members to groups.

Procedure

1. Click the  icon to create a new group or select a group from the Group Builder table and click the  icon to edit an existing group.
2. Select the Members tab of the Create new group or Edit group dialog.
3. Populate the group using one of the following methods:
 - Use the  icon to manually define group members.
 - Use the Import menu to add group members using one of the following methods:
 - From CSV
 - From group
 - From external datasource
 - From query
 - From LDAP

Restriction: The following restrictions apply when importing group members using Members tab > Import > From query or Import > From external datasource:

- When using Run Once Now, the maximum number of imported members is 5,000 rows. This is not configurable.
- When using a schedule, the maximum number of imported members is 20,000 rows by default. You can configure this limit with the CLI command **show/store populate_from_query_maxrecs**. For more information, see [Configuration and Control CLI Commands](#).

Tip: After the group is configured, import actions that can be scheduled appear as tabs on the Create new group or Edit group dialog. One-time actions such as Import from CSV cannot be scheduled and do not introduce a new tab to the dialog.

- Some group types also support advanced methods for populating groups, including the following:

- Using stored procedure analysis on datasources
- Using database dependencies
- Using reverse dependencies
- Using observed procedures
- Generating selected objects

Note: Advanced import actions are invoked on a target group that is populated based on the results of analysis performed on a user-selected input group.

What to do next

Troubleshooting: Managing groups with more than 1 million members consumes significant system memory. If you need to import, load, edit, or save very large (1 million or more members) groups, make sure that the following resources are available:

- Linux/UNIX- 2GB of free memory per million group members.
- Windows - 500MB of free memory per million group members.

If you have insufficient free memory you might experience inexplicable problems such as UI hangs, Chrome crashes, or the following error message Operation could not complete due to database error.

- [Importing from external datasources](#)

Learn how to quickly populate Guardium groups with data from your own databases and keep those groups in sync with your data.

Importing from external datasources

Learn how to quickly populate Guardium groups with data from your own databases and keep those groups in sync with your data.

About this task

Using Import > From external datasource automates the creation of custom tables, domains, and queries to populate Guardium groups from your own datasources. Once created, these artifacts represent a durable connection between Guardium and your data: updates to your data become reflected in the associated Guardium groups.

Restriction: The following restrictions apply when importing group members using Members tab > Import > From external datasource:

- When using Run Once Now, the maximum number of imported members is 5,000 rows. This is not configurable.
- When using a schedule, the maximum number of imported members is 20,000 rows by default. You can configure this limit with the CLI command **show/store populate_from_query_maxrecs**. For more information, see [Configuration and Control CLI Commands](#).

Procedure

1. Select Import > From external datasource to open the Import from external datasource dialog.
2. Use the Datasource menu to import data from a datasource.
Click the icon to define a new datasource or the icon to edit an existing datasource.
3. Use the Table name and Column name fields to identify the location of data to import from your datasource.
4. Click OK to continue.

Results

Completing the Import from external datasource dialog automatically creates or updates the following Guardium artifacts:

- Custom table
- Custom datasource
- Custom domain
- Custom query
- Group

These artifacts are available through standard Guardium tools using naming conventions described in the following table, where [table name] and [column name] are taken from the Table name and Column name fields of the Import from external datasource dialog.

Table 1. Import from external datasource: summary of artifacts created.

Artifact	Guardium tool	Naming convention	Example	Scheduled
Custom table	Custom Table Builder > Edit Data	[table name]_[column name]_[datasource ID]	USERS_ADMIN_12345	
Custom datasource	Custom Table Builder > Upload Data	[datasource name]_[datasource type](Custom Domain)	user_repository(Custom Domain)	
Custom domain	Custom Domain Builder	[group type]_[table name]_[column name]_[datasource ID]	USERS_USERS_ADMIN_12345	
Custom query	Custom Query Builder	[group type]_[table name]_[column name]_[datasource ID]	USERS_USERS_ADMIN_12345	

Artifact	Guardium tool	Naming convention	Example	Scheduled
Group	Group Builder Populate from Query		PCI Admin Users	

Attention: Imported names are truncated after 64 characters.

Using groups in queries and policies

Short overview of conditional operators for queries and where to use groups in policies.

Queries

Queries use conditional operators with groups. Here are examples of each conditional operator:

- IN GROUP - If the value matches any member of the selected group, the condition is true. IN ALIASES GROUP, this operator works on a group of the same type as IN GROUP, however assumes the members of that group are aliases. Note that the IN GROUP/IN ALIASES GROUP operators expect the group to contain actual values or aliases respectively. The Query-Report Builder will look for records with database values matching the aliases value in the group.
- NOT IN GROUP - If the value does not match any member of the selected group, the condition is true. NOT IN ALIASES GROUP, this works on a group of the same type as NOT IN GROUP, however assumes the members of that group as aliases.
- IN DYNAMIC GROUP - If the value matches any member of a group that will named as a run-time parameter, the condition is true. IN DYNAMIC ALIASES GROUP, this works a group of the same type as IN DYNAMIC GROUP, however assumes the members of that group as aliases.
- NOT IN DYNAMIC GROUP - If the value does not match any member of a group that will named as a run-time parameter, the condition is true. NOT IN DYNAMIC ALIASES GROUP, this works a group of the same type as NOT IN DYNAMIC GROUP, however assumes the members of that group as aliases.

Note: The group may contain either aliases or actual values according to the operator used (IN GROUP OR IN ALIASES GROUP) can not be used at the same time.

- LIKE GROUP - If the value is like any member of the selected group, the condition is true. This condition enables wildcard (%) characters in the group member names.

Note: A like member value uses one or more wildcard (%) characters, and matches all or part of the value. For a like comparison, alphabetic characters are not case sensitive. For example, %tea% would match tea, TeA, tEam, or steam.

Policies and rules

When creating a rule as part of a policy, groups simplify the process of specifying the parameters you want.

Anywhere there is a Group drop-down menu on the rule definition pane you can select a group.

Further, if you want to create or modify a group on the fly, click the Groups icon to open a Group Definition window and make your desired changes.

For example: if you want to capture activity occurring on your production servers, rather than typing in full IP addresses each time, you could create a group *Production Servers* and use that.

Example: Using groups to create rules and policies

Use groups to quickly specify rule conditions in a policy.

About this task

Each policy is composed of one or more rules. Specify which conditions will enact a rule, and then choose one or more actions to take when that rule is triggered. This example shows you how to use groups to identify unauthorized users, log details of their access on a group of sensitive objects, and send an alert indicating that the access occurred.

Procedure

1. Login to your Guardium system, and open the Policy Builder by clicking **Setup > Tools and Views > Policy Builder for Data**.
2. Create a new policy by clicking the icon to open the Policy Definition window.
3. Define the policy definition, then click **Apply** to save the policy.
4. Click **Edit Rules** to open the Policy Rules window and begin adding rules to the policy.
5. Click **Add Rules > Add Access Rule** to add a new rule to the policy.
6. Begin by providing a Description for the rule. Optionally provide Category and Classification labels.
7. Specify where to look for data. From the Server IP row, select the (Public) PCI Authorized Server IPs group.
The rule will apply to all activity from all PCI servers.
Note: You can view the members of any group or modify any group by going to the Group Builder.
8. Specify unauthorized users. From the DB User row, mark the Not check box and select the (Public) Authorized Users group.
The rule will apply to all users who are not in the (Public) Authorized Users group.
9. Specify sensitive objects. From the Object row, select the (Public) PCI Cardholder Sensitive Objects group.
The rule will now apply to all unauthorized users on PCI servers looking to access PCI sensitive objects.
10. Add an action to the rule by clicking **Add Action** and selecting **Action > LOG FULL DETAILS** from the menu. Click **Apply** to save the rule.
This action logs details of the access, including an exact timestamp of the access.
11. Add another action to the rule by clicking **Add Action** and selecting **Action > ALERT ONCE PER SESSION** from the menu. Specify an alert destination, then click **Apply** to save the rule.
This action sends or logs an alert indicating that the rule was triggered.
12. Click **Save** to save the rule.
13. Install the policy.
 - a. Find the policy that you created. Click Back twice, or click Policy Builder to get to the Policy Finder and browse the list of policies.

- b. With the policy selected, choose Install & Override from the installation action menu.
 c. Click OK to confirm the policy installation, and then check Latest Logs and Violations to verify the policy was installed.
 The policy is now installed and active. Any person not in the *(Public) Authorized Users* group attempting to access an object in the *(Public) PCI Cardholder Sensitive Objects* groups will have their session logged and will trigger an alert indicating the access.

Predefined Groups

This section details the predefined groups in Guardium®.

The following table describes the predefined groups that are included with your Guardium system. To view the list of all groups, open the Group Builder by clicking [Setup > Group Builder](#). Select **SQL_APP_NAME** from the Applications menu, and click Next. From the next screen, manage members from Selected Groups. The term *Group Type* refers to expectations on the type of data designated by the label. For example, the group type *Server IP* expects data arranged as an IP address (192.168.1.0) and the group type *Users* expects to see names of users of the application.

Additional predefined groups do get added periodically and these additional predefined groups may not be described here. Open the Group Builder to see all existing groups.

Predefined groups of group type DB User/DB Password are allowed only to users with the role of admin. Users can, if preferred, add other roles or even allow the groups to all roles.

Table 1. Predefined Groups

SQL_APP_NAME	GROUP_DESCRIPTION	MEMBERS
DB2® zOS Groups	zOS Audit Dynamic SQL	Group Type for DB2 commands
DB2 zOS Groups	zOS Audit Query	Group Type for DB2 commands
DB2 zOS Groups	zOS Audit Updates	Group Type for DB2 commands
DB2 zOS Groups	zOS Audit Deletes	Group Type for DB2 commands
DB2 zOS Groups	zOS Audit Inserts	Group Type for DB2 commands
DB2 zOS Groups	zOS Audit Utilities	Group Type for DB2 commands
DB2 zOS Groups	zOS Audit Object Maintenance	Group Type for DB2 commands
DB2 zOS Groups	zOS Audit User Maintenance	Group Type for DB2 commands
DB2 zOS Groups	zOS Audit User Authorization Changes	Group Type for DB2 commands
DB2 zOS Groups	zOS Audit DB2 Commands	Group Type for DB2 commands
DB2 zOS Groups	zOS Audit Plan/ Package Maintenance	Group Type for DB2 commands
IMS zOS Groups	zOS IMS Audit Query	Group Type for IMS commands
IMS zOS Groups	zOS IMS Audit Updates	Group Type for IMS commands
IMS zOS Groups	zOS IMS Audit Deletes	Group Type for IMS commands
IMS zOS Groups	zOS IMS Audit Inserts	Group Type for IMS commands
IMS zOS Groups	zOS IMS Audit DB Commands	Group Type for IMS commands
Policy Builder	Cardholder Objects	Group Type, Objects
Policy Builder	Financial Objects	Group Type, Objects
Policy Builder	PHI Objects	Group Type, Objects
Policy Builder	Authorized Client IPs	Group Type, Client IP
Policy Builder	Production Users	Group Type, Users
Policy Builder	PII Objects	Group Type, Objects
Policy Builder	Production Servers	Group Type, Server IP
Policy Builder	Financial Servers	Group Type, Server IP
Policy Builder	Functional Users	Group Type, Users
Policy Builder	Sharepoint Servers	Group Type, Server IP

SQL_APP_NAME	GROUP_DESCRIPTION	MEMBERS
Security Assessment Builder	DB2 Database Version+Patches Informix® Database Version+Patches MS Sql Server Database Version+Patches MySQL Database Version+Patches Netezza® Version+Patches Oracle Database Version+Patches Postgress Version+Patches Sybase Database Version+Patches Teradata PDE Version+Patches Teradata TDBMS Version+Patches Teradata TDGSS Version+Patches Teradata TGTW Version+Patches	Used for (specific) database version and patch level tests.
Security Assessment Builder	DB2 Allowed Grants to Public Informix Allowed Grants to Publics MS-SQL Allowed Grants to Public MYSQL Allowed Grants to Public Netezza Allowed Grants to Public Oracle Allowed Grants to Public Postgres Allowed Grants to Public Teradata Allowed Grants to Public	TUPLE, Object/Command Application 8 (Security assessment) List of objects/commands for which grants to public are allowed. These objects will be skipped on MS-SQL and Sybase tests that check grants to public. Note: Exceptions group can contain a regular expression or just a member. If regular expression, the group member must start with (R) (case sensitive), and the records in the detail will be checked against the regular expression after the (R). For example if a group member is: (R)SYSTEM.[a-z]+ each detail record will be checked using pattern: SYSTEM.[a-z]+ If the member does not start with (R) the detail record will be considered an exception only if it is equal to the group member. Note a group may contain a mix of regular expressions and specific exceptions.
Security Assessment Builder	MS-SQL Extended Procedures Allowed	Group Type is Objects
Security Assessment Builder	MS-SQL Database Administrators	Group Type is Users
12.1 and later Security Assessment Builder	MS-SQL Exclude Databases	Database names to exclude
Security Assessment Builder	Teradata Profile	Group Type is Objects
Public	Account Management Commands	Commands used to maintain accounts (users, roles, permissions), examples: REVOKE, GRANT, ALTER/CREATE/DROP USER
Public	Account Management Procedures	Account Management Objects, stored Procedures used to maintain accounts (users, roles, permissions)
Public	Active Users	Group Type is Users

SQL_APP_NAME	GROUP_DESCRIPTION	MEMBERS
Public	Admin Users	Default administrative users (DBAs and SysAdmins)
Public	Administration Objects	Privileged Objects, objects that only DBA or Sys Accounts should access. These accounts are locked for "public" by default.
Public	Administrative Commands	Privileged Commands, privileged Commands, should be executed only by DBAs. Examples: GRANT, BACKUP, DDL commands
Public	Administrative Programs	Database utilities (clients) that come with database and usually reside on the database server and could be used by the server itself
Public	ALTER Commands	Examples, alter database, alter procedure, alter profile, alter session, alter user
Public	Application Privileged Commands	Public privileged commands that should be revoked from "public", but not revoked since they are used by the application
Public	Application Privileged Procedures	Application Privileged Objects, public privileged procedures that should be revoked from "public" but not revoked since they are used by the application
Public	Application Schema Users	Application Users, database user used by the application to maintain/user the application tables
Public	Archive Candidates	Group Type is Objects
Public	Authorized Source Programs	Group Type is Source Programs
Public	Authorized Users	Group Type is Users
Public	Connection Profiling List	Group Type is Client IP/Src App/DB User/Server IP/SVC. Name List of allowed connections
Public	CREATE Commands	Examples, create context, create database link, create function, create statistics, create type, create user
Public	Credentials Related Entities	Guardium Audit Types, Self-Monitoring, examples, allowed_role, LDAP_config, Turbine_user_group_role
Public	Data Transfer Commands	Backup Commands, commands dealing with backup/restore of database data
Public	Data Transfer Procedures	Data Transfer Objects, procedures dealing with backup/restore of database data (mostly on MSS and SYB)
Public	DB Predefined Users	Either non-admin predefined users or all predefined users, including administrative ones
Public	DBCC Commands	Group Type is Commands
Public	DDL Commands	Data Definitions Language, schema-privileged commands, examples, ALTER, CREATE, DROP
Public	DML Commands	DML Commands, examples, insert, truncate, update
Public	DROP Commands	Examples, drop_context, drop_event_monitor, drop_procedure, drop_role
Public	DW All Object-Field DW All Objects DW Execute Accessed Objects DW Select Accessed Objects DW Select Accessed Objects/Fields	There are five predefined reports that use monitored data to show object names. These reports all start with the prefix DW (Data Warehouse). See the help topic, How to report on dormant tables/columns, for further information on how to use these predefined reports.
Public	EBS App Servers	Group Type is Client IP
Public	EBS DB Servers	Group Type is Server IP
Public	EXECUTE Commands	Examples, call, execute, execute function
Public	GRANT Commands	Examples, grant, grant objectives, grant system privileges
Public	Guardium Audit Categories for Detailed Reporting	Guardium patches, TURBINE_USER_GROUP_ROLE
Public	ICM App Servers	Group Type is Client IP
Public	ICM DB Servers	Group Type is Server IP
Public	ImportLDAPUser	Group Type is Objects
Public	ImportLDAPUser_bin dValues	Group Type is Objects
Public	Inspection Engine Entities	Examples, adminconsole_sniffer, software_tap_db_client, software_tap_db_server
Public	Java™ Commands	Examples, alter java, create java, drop java
Public	KILL Commands	Example, kill
Public	Masked_SP_Executio ns_MS_SQL_SERVER	For MS SQL Server, a group that includes a collection of stored procedures (SP) names. If there is an execution of an included procedure, than everything will be masked, even if in quotes. Predefined as empty.
Public	Masked_SP_Executio ns_Sybase	For Sybase, a group that includes a collection of stored procedures (SP) names. If there is an execution of an included procedure, than everything will be masked, even if in quotes. Predefined as empty.
Public	MongoDB Skip Commands	Group Type is Commands
Public	MS-SQL Replication Procedures	Group Type is Objects
Public	MS-SQL Security System Procedures	Group Type is Objects

SQL_APP_NAME	GROUP_DESCRIPTION	MEMBERS
Public	MS-SQL System Procedures	Group Type is Objects
Public	Oracle EBS HRMS Sensitive Objects	Group Type is Objects
Public	Oracle EBS-PCI	Group Type is Objects
Public	Oracle EBS-SOX	Group Type is Objects
Public	Oracle Predefined Users	Group Type is Users
Public	Peer Association Commands	Commands dealing with links/replications of data, examples, links, log shipping, replications, snapshots
Public	Peer Association Procedures	Peer Association Objects, procedures dealing with links/replications of data Examples: Links, log shipping, replications, snapshots
Public	PeopleSoft Objects	Group Type is Objects
Public	PeopleSoft Sensitive Objects	Group Type is Objects
Public	Performance Commands	Examples, analyze, create statistics, update all statistics
Public	Policy Related Entities	Examples, access_rule, gdm_install_policy_header
Public	Potential Overflow Objects	Group Type is Objects
Public	Procedural Commands	Examples, begin, call, execute, exit, repeat, set
Public	PROCEDURE DDL	Examples, alter procedure, create procedure, drop procedure
Public	PSFT App Servers	Group Type is Client IP
Public	PSFT DB Servers	Group Type is Server IP
Public	Public executable procedures	Execute-Only Objects, procedures/functions/Packages that by default granted access to public
Public	Public selectable object	Select-only Objects, tables that by default granted access to public
Public	RESTORE Commands	Examples, restore database, restore log
Public	REVOKE Commands	Examples, revoke object privileges, revoke system privileges
Public	Risk-indicative Error Messages	SQL errors related to security
Public	Sharepoint Servers	
Public	SAP-PCI	Group Type is Objects
Public	SAP App Servers	Group Type is Client IP
Public	SAP DB Servers	Group Type is Server IP
Public	SAP HR Sensitive Objects	Group Type is Objects
Public	Select Command	Examples, select, select list
Public	Sensitive Objects	Examples, activity, sales
Public	SIEBEL App Servers	Group Type is Client IP
Public	SIEBEL DB Servers	Group Type is Server IP
Public	Siebel SIA Sensitive Objects	Group Type is Objects
Public	SPECIAL CASE Source Program	Group Type is Source Programs
Public	Suspicious Objects	Group Type is Objects
Public	Suspicious Users	Group Type is Users
Public	System Configuration Commands	Database configuration commands (subset of Administrative Commands) Examples: ALTER DATABASE, ALTER SYSTEM
Public	System Configuration Procedures	System Configuration Objects (subset of Administration Objects)
Public	Terminated DB Users	Group Type is Users
Public	Vulnerable Objects (with wildcards)	Database objects with reported vulnerabilities

SQL_APP_NAME	GROUP_DESCRIPTION	MEMBERS
Public	DB2 Default Users IBM iSeries Default Users Informix Default Users MS-SQL Server Default Users MYSQL Default Users Netezza Default Users Oracle Default Users PostgreSQL Default Users Sybase Default Users Teradata Default Users	Group Type is DB User/DB Password
Public	Hadoop Skip Commands Hadoop Skip Objects Not Hadoop Server	Group Type is Command Group Type is Object Group Type is Server IP
Public	Replay - Exclude from Compare Replay - Include in Compare	Group Type is Objects
Audit Process Builder		Predefined as empty.
Classifier		Predefined as empty.
Express Security		Predefined as empty.

Security Roles

Security roles are used to grant access to data (groups, queries, reports, etc.) and to grant access to applications (Group Builder, Query-Report Builder, Policy Builder, CAS, Security Assessments, etc).

By default, when a component is initially defined, only the owner (the person who defined it) and the admin user (who has special privileges) are allowed to access and modify that component.

You can allow other users to access the components you define by assigning security roles. For example, if you assign a security role named DBA to an audit process, all users assigned the DBA role will be able to access that audit process.

Note: In order to configure LDAP user import, accessmgr user must have the privilege to run the Group Builder. In certain situations, when changes are made to the role privilege, accessmgr's privilege to Group Builder can be taken away. This results in an inability to save or run successfully LDAP user import. Go to the access management portal, select Role Permissions. Choose the Group Builder application and make sure that there is a checkmark in the all roles box or a checkmark in the accessmgr box.

Assign Security Roles

1. Open or select the item to which you want to assign one or more security roles (a policy or report definition, for example).
2. Click Roles.
3. Check all of the roles you want to assign from the Assign Security Roles list. You can only assign roles that are assigned to your account.
4. Click Apply.

Define a new Security Role

By default, only the special accessmgr user is allowed to create or remove security roles.

1. Login as accessmgr and open the User Role Browser by clicking Access > Access Management > User Role Browser.
2. At the end of the role browser, click Add Role.
3. In the Role Form panel, enter a new Role Name and click Add Role.

Remove a Security Role

By default, only the special accessmgr user is allowed to create or remove security roles. To remove a role assigned to a component, see Assign security roles to a component.

1. Login as accessmgr and open the User Role Browser by clicking Access > Access Management > User Role Browser.
2. Click Delete for any role, and then click Confirm Deletion.

How to install patches

Install a single patch or multiple patches as a background process.

About this task

Use this topic to provide visibility and control over patch installation, status and history. See Central Management for more information.

This how-to topic uses a combination of commands from the CLI and choices from the GUI to help you install the latest Guardium patch. The Guardium system must be rebooted after installing a patch.

Important: Patches downloaded in ZIP format must be unzipped outside the Guardium® system before uploading and installing. Observe the following restrictions for any patch with database structure changes:

- Perform or schedule the patch installation during quiet time on the Guardium system to avoid conflicts with long-running processes such as heavy reports, audit processes, backups, and imports.
- The exact time required for patch installation depends on database utilization, data distribution, and other considerations.
- Install patches in a top-down manner, first patching a central manager before patching aggregators and finally collectors.

In the procedure below, you will follow these steps from the Guardium system that is designated and configured as the Central Manager:

1. Enter the CLI command **store system patch install** to install a single patch or multiple patches to the Central Manager from a network location.
2. Click Setup > Tools and Views > Patch Distribution to move patches from the CM to managed units.

Procedure

Install the patch(es) to the Central Manager

Note: A compressed patch file may contain multiple patches, but only one patch can be installed at a time. To install more than one patch, choose all the patches that need to be installed, separated by commas. Internally the CLI submits requests for each patch on the list (in the order specified by the user) with the first patch taking the request time provided by the user and each subsequent patch three minutes after the previous one. In addition, CLI will check to see if the specified patch(es) are already requested and will not allow duplicate requests.

1. Enter the following command:

```
store system patch install <type> <date> <time>
```

where **<type>** is **sys**, **ftp**, **scp**, or **cd** and **<date>** and **<time>** are the patch installation request date and time formatted as YYYY-mm-dd and hh:mm:ss. If date and time are not entered or if "now" is entered, the installation request time is NOW.

Table 1. Patch install type descriptions and parameters

Name	Description
sys	The sys option is for use when installing a second or subsequent patch from a compressed file that has been copied to the Guardium system by using this command previously. Use this option to apply a second or subsequent patch from a patch file that has been copied to the IBM® Guardium system by a previous store system patch execution. Install from /var/log/guard/patches
ftp or scp	The ftp and scp options copy a compressed patch file from a network location to the Guardium system. To install a patch from a compressed patch file located somewhere on the network, use the ftp or scp option, and respond to the prompts as shown below. Important: Patches downloaded in ZIP format must be unzipped outside the Guardium system before uploading and installing. Observe the following restrictions for any patch with database structure changes: <ul style="list-style-type: none"> • Perform or schedule the patch installation during quiet time on the Guardium system to avoid conflicts with long-running processes such as heavy reports, audit processes, backups, and imports. • The exact time required for patch installation depends on database utilization, data distribution, and other considerations. • Install patches in a top-down manner, first patching a central manager before patching aggregators and finally collectors. Please enter the following information for file transfer: Host to import patch from: User on (host name): Full path to the patch, including name (file name may use wildcard *): (LDAP Password) Password: Enter the scp/ftp port if you need to use a special port, else just press Enter key to continue: The file transfer process can take a while to complete. Leave the terminal open and do not answer any questions until the transfer is complete. Starting transfer, please wait. The file transfer is complete. Do you want to continue (yes or no)? yes List the files in the patches directory: 1. (name of file) Please choose patches to install (1-1, or multiple numbers separated by ",", or q to quit): 1 Install item 1 Patch has been submitted, and will be installed according to the request time, please check installed patches report or CLI (show system patch installed). Please don't forget to remove your media if necessary.

Name	Description
<code>cd</code>	<p>The <code>cd</code> option is for use in installing the patch from a DVD disk. To display a complete list of applied patches, see the Installed Patches report on the Guardium Monitor tab of the administrator portal. There is also an Available Patches report on this same Guardium Monitor tab. To install a patch from a DVD, insert the DVD into the IBM Guardium DVD ROM drive before executing this command. A list of patches contained on the DVD will be displayed.</p> <ul style="list-style-type: none"> To delete a patch install request, use the CLI command <code>delete scheduled-patch</code> Patches remain after installation only on the Central Manager. Standalone or managed unit patch files ARE deleted after installation. To display the available patches: <code>show system patch available</code> To display the already installed patches and patches scheduled to be installed—showing date/time and the install status: <code>show system patch installed</code> Use the <code>fileserver</code> command to start an HTTPS-based file server running on the Guardium appliance. This facility is intended to ease the task of uploading patches to the unit, or downloading debugging information from the unit. Each time this facility starts, it deletes any files in the directory to which it uploads patches. <p>Note: Any operation that generates a file, that the fileserver will access, should finish before the fileserver is started (so that the file is available for the fileserver).</p> <ul style="list-style-type: none"> To start the file, enter the fileserver command: <code>fileserver</code> Starting the file server. You can find it at <code>https://(name of unit)</code> Press ENTER to stop the file server. Open the fileserver in a browser window, and to one of the following: <ul style="list-style-type: none"> To upload a patch, click Upload a patch and follow the directions. To download log data, click Sqlguard logs, go to the file you want, right-click on it, and download as you would any other file. When you are done, return to the CLI session and press Enter to terminate the session.

Use the UI to move the patch(es) from Central Manager to managed units

2. Navigate to `Manage > Central Management > Central Management`.
 3. From the Central Management page, select managed units to receive the patch and click the Patch Distribution button.
 4. From the Patch Distribution page, select the patches to distribute.
- The Patch Distribution page displays an available patch list with dependencies, and allows for the selecting of a patch and installing it to all selected units. The list of available patches is constructed out of the available patches and evaluating the currently installed patches on each of the selected units along with the dependency list of available patches. Patches available but not installable (a dependent patch is missing) are shown in the list as grayed out and cannot be selected. The selection of patch to install is a single selection: only one patch can be installed at a time.
- Click Install Patch Now to install the patch immediately.
 - Click Schedule Patch to schedule patch installation for the future.
- After clicking Install Patch Now, a command is sent to all selected units to install that patch. The process of installing patches happens in the background.
5. Navigate to `Central Management > Central Management > Patch Distribution`.
 6. Click on Patch Installation Status. The Patch Installation Status screen will display for each unit, failed installations and discrepancies - situations such as having one patch being installed on part of the units only, regardless if it failed on other units or was not installed.

Results

The patched systems are now ready to be used; however, remember that the Guardium system must be rebooted after installing a patch.

Support Maintenance

The Support Maintenance feature is password protected and can be used only as directed by Technical Support. Contact Technical Support if you require more information.

Product integration

You can integrate IBM® Guardium® with other products.

- [Configure BIG-IP Application Security Manager \(ASM\) to communicate with Guardium system](#)
Use the Big-IP ASM (from F5 Networks) together with Guardium's real-time database activity monitoring to solve the problem of identity propagation between web application and database application server layers.
- [Embedded integrations](#)
You can use available integrations with Guardium UNIX and Linux® systems.
- [Integrating with IBM Knowledge Catalog for federated data protection](#)
You can enable federated data protection to integrate your IBM Knowledge Catalog service with Guardium Data Protection to help ensure that data protection rules that are defined in IBM Knowledge Catalog are enforced at the data source-level in a consistent way across in-scope data sources. To enable federated data protection, use Guardium query rewrite capabilities to create and run transformations (such as data masking) that are based on IBM Knowledge Catalog rules.
- [PIM Integration with Guardium DAM](#)
Privileged Information Management (PIM) helps organizations to automate and track the use of shared privileged identities and monitor the usage of these shared privileged identities.
- [Configuring an external ticketing system](#)
Use an external ticketing system such as ServiceNow or IBM Resilient to track incidents, problems, and tasks discovered by Guardium.
- [Configuring vulnerability scanner agents](#)
Common Vulnerabilities and Exposures (CVE) scanner agents, such as Nessus and Qualys, gather information about the Guardium system and send it to their third-party portal, which analyzes and generates reports. If the agent can run as root directly on the Guardium system, the resulting report is much more accurate with fewer false positive results. Use `scanner_agent` CLI commands to install and manage root access to CVE scan tools.
- [QRadar and Guardium integration](#)
QRadar and Guardium can work together in a two-way information flow to have the Guardium data protection policies updated automatically and nearly in real-time

- in response to security intelligence events from QRadar.
- **[OPTIM to Guardium Interface](#)**
An OPTIM to Guardium interface, using Protobuf (Universal Feed Agent), sends Optim activity logs to Guardium.
 - **[Combining real-time alerts and correlation analysis with SIEM products](#)**
Distribute contextual knowledge of database activity patterns, structures, and protocols directly to the third-party database of the SIEM system.
 - **[CEF Mapping](#)**
The CEF standard from ArcSight defines a set of required fields, and a set of optional fields.
 - **[LEEF Mapping](#)**
Log Event Extended Format (LEEF) from QRadar

Configure BIG-IP Application Security Manager (ASM) to communicate with Guardium system

Use the Big-IP ASM (from F5 Networks) together with Guardium's real-time database activity monitoring to solve the problem of identity propagation between web application and database application server layers.

This solution uses Google's protocol buffers (.protobuf) as the wire format between BIG-IP ASM and the Guardium® system.

Information about configuring the integration between Big-IP ASM and the Guardium real-time database activity monitoring is provided by [Deploying the BIG-IP LTM with Guardium](#).

Embedded integrations

You can use available integrations with Guardium® UNIX and Linux® systems.

Db2 Warehouse integration

Guardium is integrated into Db2® Warehouse. For more information about integrating a Guardium collector with Db2 Warehouse, see [Configuration options](#) in the *IBM Docs for the Integrated Analytics System*.

Netezza Performance Server (NPS) integration

Guardium is integrated into Netezza® Performance Server. For more information about integrating Guardium with NPS®, see [Enabling query and result sharing with Guardium](#) in the IBM® Docs for the *IBM Netezza Performance Server*.

Integrating with IBM Knowledge Catalog for federated data protection

You can enable federated data protection to integrate your IBM® Knowledge Catalog service with Guardium® Data Protection to help ensure that data protection rules that are defined in IBM Knowledge Catalog are enforced at the data source-level in a consistent way across in-scope data sources. To enable federated data protection, use Guardium query rewrite capabilities to create and run transformations (such as data masking) that are based on IBM Knowledge Catalog rules.

Before you begin

The integration between Guardium and IBM Knowledge Catalog is available for data sources that have data source-specific user-defined functions (UDFs) available. To use the IBM Knowledge Catalog for federated data protection, you must install the UDF for your data source.

To integrate the Guardium query rewrite with IBM Knowledge Catalog transformation, you need:

- IBM Cloud Pak® for Data 4.6 or later with IBM Knowledge Catalog service.
Note: IBM Knowledge Catalog works with the Cloud Pak for Data Data Privacy service to provide masking and transformation. Before you can use this integration, you need to enable both the IBM Knowledge Catalog and the Data Privacy service. Be sure to check the [Known issues for Data Privacy \(Masking flow\)](#) in the IBM Docs for Cloud Pak for Data for any issues that you might need to know about.
- The IBM Knowledge Catalog - Guardium integration must be running.
- One or more users with privileges to run Cloud Pak for Data data protection rules. The users do not need to be admins.
- Guardium Data Protection 11.5 or later.
- A supported data source for which a set of user-defined functions is available along with the user-defined functions for your data source. User-defined functions are precompiled into libraries that are suitable for each data source. For more information about supported data sources and UDFs, see [Adding User-Defined Functions \(UDFs\) for IBM Knowledge Catalog - Guardium integration](#).

Architecture notes

How the IBM Knowledge Catalog - Guardium integration works (IBM Knowledge Catalog view)

The integration adds the policy enforcement point (PEP) from the IBM Knowledge Catalog XACML model. The PEP allows Guardium to use IBM Knowledge Catalog rules for enhanced data protection.

In IBM Knowledge Catalog, a PEP cache stores evaluation responses (decisions) that are received from IBM Knowledge Catalog data protection rules. Each decision is an instance of a computed outcome that is based on a combination of the current policy space and user context.

How transformation integration works (Guardium view)

From a Guardium perspective, the transformation integration takes the following steps:

For more information, see [Column alias parameter](#).

Maximum of 2 conditions for row-level filtering

For row-level filtering, you can include up to two conditions in your IBM Knowledge Catalog query. For more information, see [Setting up a transformation integration](#).

- [Starting the IBM Knowledge Catalog and Guardium Data Protection integration](#)

After your Guardium and IBM Knowledge Catalog systems are correctly configured, you can configure and start the integration from the Guardium UI.

- [Setting up a transformation integration](#)

After the IBM Knowledge Catalog - Guardium integration is working, you can integrate Guardium query rewrite functionality with IBM Knowledge Catalog and the Cloud Pak for Data Data Privacy service to provide masking and transformation for specified data sources.

Related information

- [store certificate wkc](#)
 - [store wkc configuration](#)
 - [Adding User-Defined Functions \(UDFs\) for IBM Knowledge Catalog - Guardium integration](#)
-

Starting the IBM Knowledge Catalog and Guardium Data Protection integration

After your Guardium® and IBM® Knowledge Catalog systems are correctly configured, you can configure and start the integration from the Guardium UI.

Before you begin

Before you begin, store the IBM Cloud Pak® for Data root certificate on any managed units or stand-alone machines. For more information about storing the Cloud Pak for Data certificates, see [store certificate wkc](#).

Note: Do not use the self-signed certificate that is installed with Cloud Pak for Data. Always use a certificate authority (CA)-signed certificate in production environments.

Procedure

1. To set up policy integration on a Guardium central manager, browse to Protect->Security Policies->Policy Builder for Data.
2. From the Security Policies page, open the Configure WKC window.
 - From a central manager, select Configure WKC.
 - From a stand-alone machine, click Manage, and then select Configure WKC.
3. From the WKC configuration page, enter the following information:
 - Enable WKC data protection rules - Toggle to use IBM Knowledge Catalog data protection.
 - WKC service URI - The URI of the IBM Knowledge Catalog service.
 - Credential type- Select a method to manage credentials:
 - Assign credentials - If you choose to assign credentials, then supply your IBM Knowledge Catalog User name and User password.
 - External password - To support an external credential manager, such as AWS Secrets Manager or CyberArk, select External password, and then select one of the credential managers from the list. Enter the requested information for that credential manager.

Note: If the credential manager password changes, use the [wkc_refresh_external_pwd](#) API to update the password.

- User scope - The owner of this asset. Select either Database user (the default) or Application user. For more information, see [How the Guardium default user works](#).
- Column alias - With column-level transformation, SQL column fields can be transformed by some long IBM Knowledge Catalog UDF function calls. Use Column alias to specify whether to use the original column names or an alias of the function name, which can be shorter and help hide some transformation details (which might provide extra security).

As the database server evaluates the transformed SQL, the transformed function signature displays as the column name in the database client.

For example, using the following input query:

```
select EmpCard from EMPLOYEE
```

You can select one of the following options for how to display the transformed query in the database client.

- Use original column name - Use the original COLUMN_NAME as the IBM Knowledge Catalog UDF alias. The transformed query includes the original column name and the actions taken. The transformed query displays as follows:

```
select WKC.MASK_STRING(0, "XXXXXXXXXX", ". ", EmpCard) AS EmpCard from EMPLOYEE;
```

- Use full function signature - Do not use an alias for the column-transformation UDF. The transformed query displays as follows:

```
select WKC.MASK_STRING(0, "XXXXXXXXXX", ". ", EmpCard) from EMPLOYEE;
```

- Use short function signature - Use the MASKFUNCTIONNAME_COLUMNNAME as the UDF alias. The transformed query includes the masked function name and the original column name. The transformed query displays as follows:

```
select WKC.MASK_STRING(0, "XXXXXXXXXX", ". ", EmpCard) AS MASK_STRING_EmpCard from EMPLOYEE;
```

Regardless of which alias option you select, if the column name in the SQL query statement has a defined alias, then the aliases in the SQL statement are preserved by query rewrite. The column alias option is only available if the SQL column without an alias triggers any column-level transformation.

- Action on unexpected response - Deny is the default. Select Allow to allow the connection.

If Guardium receives an unexpected response (or no response) from IBM Knowledge Catalog, you can choose to allow or deny the connection to IBM Knowledge Catalog. The default is Deny, that is, treat the connection as a IBM Knowledge Catalog policy violation. Click Allow to allow the connection, which treats the connection as approved.

- Cache size - The size of the cache determines the maximum number of decisions that can be stored in memory at any point in time. The default is 1000 decision entries.

- Time to live (minutes) - The time-to-live (in minutes), that is, the amount of time that each decision is available, in the primary cache. After the time-to-live passes, the decision is deleted from cache. Default = 60. The maximum is 1440.
 - Enable persistent cache - If you enable persistent cache, then you must also specify the following parameters.
 - Maximum entries - The maximum number entries to save in cache. The minimum is 1. Default = 100000.
 - Maximum files - The maximum number of files to save in cache. Default = 10. The maximum is 100.
 - Time to live (days) - The time-to-live (in days) for each decision in the persistent cache. Default = 7. The maximum is 30.
4. For central managers, the Collector table displays all of the collectors that are associated with this central manager.
- a. Filter, if needed, and select the collectors to include in the IBM Knowledge Catalog integration.
 - b. Click OK to begin using the IBM Knowledge Catalog data protection rules for the central manager and selected collectors.
- Note: You can also change the parameters for collectors (and stand-alone machines) by using the [store wkc configuration](#) CLI.
5. For a stand-alone machine, click OK to begin using the IBM Knowledge Catalog data protection rules on that machine.

What to do next

After you enable the IBM Knowledge Catalog integration, the integration runs until you disable it. However, be sure to stop the integration before you add new assets to the IBM Knowledge Catalog. If the integration is running when you add assets, the new connections are denied and an error occurs.

After the integration is working, you can add transformation and other processes for specific data sources as described in [Setting up a transformation integration](#).

Setting up a transformation integration

After the IBM® Knowledge Catalog - Guardium integration is working, you can integrate Guardium® query rewrite functionality with IBM Knowledge Catalog and the IBM Cloud Pak® for Data Data Privacy service to provide masking and transformation for specified data sources.

Before you begin

To integrate Guardium query rewrite with IBM Knowledge Catalog transformation, you need:

- Cloud Pak for Data 4.6 or later with IBM Knowledge Catalog service.
Note: IBM Knowledge Catalog works with the Cloud Pak for Data Data Privacy service to provide masking and transformation. Be sure to check the [Known issues for Data Privacy \(Masking flow\)](#) in the IBM Docs for Cloud Pak for Data for any issues that you might need to know about.
- One or more users with privileges to run Cloud Pak for Data data protection rules. The users do not need to be admins.
- Guardium Data Protection 11.5 or later.
Important: Guardium query rewrite must be enabled on the S-TAP used for IBM Knowledge Catalog integration. For more information, see [Enabling query rewrite](#).
- A supported data source for which a set of user-defined functions (UDFs) is available.
- A UDF for your data source. User-defined functions are precompiled into libraries that are suitable for each data source. For more information about the supported data sources and UDFs, see [Adding User-Defined Functions \(UDFs\) for IBM Knowledge Catalog - Guardium integration](#).
- You can include up to two conditions in your IBM Knowledge Catalog query. For more information, see [Filtering rows in data protection rules \(IBM Knowledge Catalog\)](#).

About this task

After the transformation integration is set up and running, you will not see anything different. However, details about the data transformations are available in Guardium reports.

From a Guardium perspective, the transformation integration takes the following steps:

- A customer defines data protection rules in IBM Knowledge Catalog.
- Guardium sends session and request details to IBM Knowledge Catalog for evaluation in the form of a resource key.
- The verdict from IBM Knowledge Catalog is returned and can include a transformation specification that provides details about how to transform the query.
- Guardium uses its query rewrite capabilities to rewrite the query in accordance with the transformation specification.
- The altered query is forwarded to the database server by an S-TAP (or External S-TAP) and the Guardium sniffer.
- The transformed (such as pseudonymized, redacted, or anonymized) data is returned to the database client.

Procedure

1. Have both Guardium and IBM Knowledge Catalog installed and running.
2. Have your data source prepared.
3. Start the integration, as described in [Starting the IBM Knowledge Catalog and Guardium Data Protection integration](#).
4. Acquire and install the UDF for your data source. For more information, see [Adding User-Defined Functions \(UDFs\) for Watson Knowledge Catalog \(WKC\) - Guardium integration](#).
5. Create data protection rules in IBM Knowledge Catalog. You can incorporate Guardium query rewrite policy rules to provide row-level filtering. You can include up to two conditions in your IBM Knowledge Catalog query. For more information, see [Filtering rows in data protection rules \(IBM Knowledge Catalog\)](#).

Results

After the integration is running, you can view the results of the queries in Guardium reports. Create a custom report for the `GDM_QR_LOG` table.

Related information

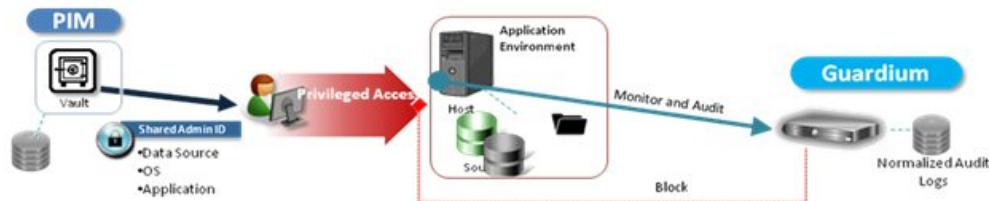
- [Adding User-Defined Functions \(UDFs\) for Watson Knowledge Catalog \(WKC\) - Guardium integration](#)
- [Data protection rules \(IBM Knowledge Catalog\)](#)

PIM Integration with Guardium DAM

Privileged Information Management (PIM) helps organizations to automate and track the use of shared privileged identities and monitor the usage of these shared privileged identities.

The idea is to integrate PIM activity data with Guardium DAM data, in order to allow visibility to the actual user (person) that logged in to the database.

The diagram illustrates the integration.



The main purpose of this integration is:

- Provide visibility in the Guardium appliances to PIM data such as Lease history (who used the shared accounts), credentials and databases managed by PIM.
- Provide DAM information correlated with PIM information, for example, Guardium can show today's Database user along with actual requests issued by a specific user. This integration will allow use of both the Database user and the actual PIM user that leased the shared ID.

Installation

Guardium patch (v10.1p103) can be used to install PIM integration functionality. PIM integration can be used on standalone Guardium systems as well as in federated environments.

Note: It is assumed that the PIM activity data is already implemented.

Follow these steps

1. Bring data to the Guardium system.

Select a datasource and then select from the Guardium UI: Reports > Report Configuration Tool > Custom Table Builder.

Locate and select three PIM predefined tables and, for each one of them, schedule Automatic Data Upload.

Upload PIM tables to Guardium System

If using a Guardium Central Manager, select from the Guardium UI: Manage > Central Manager > PIM Data Distribution. Do this to schedule data distribution from the Central Manager to all managed units.

2. Once data is brought to the managed units, use this CLI command, store pim_correlation_mode, to enable correlation of PIM data with Guardium session data.

CLI command

```
store pim_correlation_mode
```

Usage: store pim_correlation <state>

where state is on/off. On is to enable and off is to disable.

Show command

```
show pim_correlation_mode
```

3. To run correlation , select from the Guardium GUI:Comply...> Custom Reporting>PIM data correlation.

Correlated data can be seen through reports in Access domain

The screenshot shows the Guardium Query Builder interface. On the left, a sidebar lists navigation options: Welcome, Setup, Manage, Discover, Harden, Investigate, and Protect. Below this is a message: "PIM session in Access Domain". The main area is titled "Query Builder" and contains two panels. The left panel, "Entity List", has a tree view with "Client/Server" expanded, showing "PIM Session" which is circled in red. Other items include TAXIS Global Id, TAXIS Session Id, User Name, Checkout Timestamp, Checkin Timestamp, desc: Credential Tag, desc: Resource Tag, desc: Justification, GMT Checkout Timestamp, Client Server/Session, Session, Access Period, SQL, Application Events, and FULL SQL. The right panel, "PIM correlation", has a header "Main Entity: Session" and a table with columns Seq., Entity, and Attribute. Below the table is a section for "Addition mode" with radio buttons for AND, OR, and HAVING.

Configuring an external ticketing system

Use an external ticketing system such as ServiceNow or IBM Resilient to track incidents, problems, and tasks discovered by Guardium.

Before you begin

Before you can configure Guardium® for external ticketing, make sure that your ticketing system is set up.

Note: Before you configure Guardium to use external ticketing with ServiceNow, make sure that the ServiceNow Event Management Core app is available in your ServiceNow instance. You can download the Event Management Core app from the ServiceNow store.

Depending on your ticketing system and the Guardium system that you configure, you can select the mode to process ticket information, as follows.

- Table - Identifies the type of ticket that is opened on the ticketing system. Each table provides options for the selected system. For example, if you select the Vulnerability Assessment Results system, you can select the specific severity for which you want to automatically create tickets.
 - Event - For Alert and Vulnerability Assessment systems with ServiceNow, select Event to send an event to ServiceNow when a Guardium alert occurs. Upon receiving events, ServiceNow generates alerts based on ServiceNow event and alert management rules.
- No roles are required to create an event, as long as the ServiceNow user account from the Guardium external ticketing configuration has permission to connect to the ServiceNow instance.

Note: Before you configure an external ticketing system with Guardium 12.0 or later, make sure that the correct version of TLS is available. For more information, see [Managing the TLS version](#).

Procedure

- Browse to Setup...Tools and Views...External Ticketing System.
 - Click the icon to open the External Ticketing System Configuration dialog.
 - From the Account tab, use the Account menu to select an existing ticketing system account or click the icon to add an account.
 - From the Add account dialog, select, and configure your ticketing system, as follows:
 - For IBM Resilient, URL is the fully qualified domain name.
 - For ServiceNow, URL is generally `<instanceName>.service-now.com`.
- When you create the first external account, Guardium automatically creates configurations for all of the Guardium systems.
- Enter the username and password for your ticketing system, and then click Test Connection to verify that Guardium can communicate with the ticketing system.
 - Note:
 - The ticketing-system account must be able to create and read records that are used with the integration. For example, if Incident records are used, the user must be able to create and read Incident records.
 - If prompted, follow the on-screen instructions for adding a security certificate for the ticketing system: Download the certificate from the ticketing system and import it into Guardium with the `store certificate keystore trusted console` CLI command.
 - From the Settings tab, select the Guardium system to configure. Systems are specific Guardium features that support external ticketing integration.
 - Then, depending on your ticketing system and the Guardium system that you select, you can take one of the following steps:
 - For IBM Resilient, select the Guardium system that you want to configure from the Settings tab, and then select the Table to configure.
 - For ServiceNow, when you select either Risk Spotter or Threat Analytics, select the Table to configure.

If you select Table mode for ServiceNow, you also need to select the table you want to use. You can search for a table (or other items, such as an assignment group, depending on the Guardium system). To search for a specific table name or other item,

- Click the icon to open the Search page for that item.
- In the search box, enter all or part of the text for the item you want to find, and then click Search.
- Select the item that you want from the list, and click Add.



If needed, click the icon to clear the text.

When you select Vulnerability Assessment in either Event or Table mode, you can also specify the conditions for which you automatically want to create events or tickets. The conditions are defined as part of the Guardium assessment. Enter the following information in Automatically create events/tickets when these conditions are met,

- Severity - Select one or more severity settings for which to create an event or ticket. You can select as many settings as needed.
- Test result score - Select one or more result scores. You can select as many settings as needed.

For more information, see [Introducing Guardium Vulnerability Assessment](#).

8. After you select the Guardium system and Table, use the Guardium fields controls to create the message table that Guardium sends to the ticketing system. The information that you supply depends on the external ticketing system.

IBM Resilient tickets

- Name - A name or description of the external ticket type.
- Description - The Guardium fields to include in each ticket.
- Members - The member of the Resilient team to receive this ticket. A member can be either one person or a group (that is defined in Resilient). Note: In Guardium, you can select only one member. You can add more ticket receivers in Resilient.
- Incident types - Select a Resilient incident type. Note: Guardium automatically creates configurations for all four of the Guardium systems. However, the Incident type field is left blank. Since Incident type is required for Resilient tickets, you need to select an incident type for each Resilient ticket type. You can set the incident type either from the Guardium UI or the Resilient server.
- Click the icon to add a field. For IBM Resilient, you can enter comments to include with a ticket.

ServiceNow tickets

For all ticket types (Tables), you can configure some or all of the following information,

- Short description - A short description of the external ticket type.
- Description - The Guardium fields to include in each ticket
- Assignment group - The ServiceNow group to assign this ticket to.
- Click the icon to configure extra fields. For ServiceNow, you can enter comments to include with a ticket or other information (depending on the Guardium system and table). Note: ServiceNow supports both comments and work notes. Only comments entered into the ServiceNow Additional comments (customer visible) field display in the Guardium External Tickets report.

9. From the Status tab, review ticketing-related log information.

Use the Enable debug checkbox to include debugging-level information in the log.

Note: The Enable debug setting is saved when selected or cleared.

10. Click Save to save the configuration and exit the External Ticketing System Configuration dialog.

11. If needed, configure external tickets for the other available systems that are shown in the External Ticketing System table.

What to do next

After you configure ticketing integration for specific Guardium systems, use the following integration points in the Guardium UI to open new tickets.

Guardium system	Integration point
Alerter	<p>Browse to Protect > Database Intrusion Detection > Alert Builder. Configure an alert. In the Add receiver section, set Notification type to TICKET. Tickets are created when the alert triggers.</p> <p>Attention: Verify that the alerter is active on startup: browse to Setup > Tools and Views > Alerter and select the Active on startup checkbox.</p> <p>External ticketing integrates with the following types of alert notifications:</p> <ul style="list-style-type: none"> • Receivers defined in the Alert Builder • Notifications defined for a security policy in the Policy Builder for Data • Tickets defined for receivers in the Audit Process Builder.
Audit Process	<p>The audit process ticketing system uses the Alert integration point.</p> <p>Browse to Comply > Tools and Views > Audit Process Builder. Begin creating an audit process. From the Send results section, select to add a receiver, and then set Receiver Type to Ticket.</p> <p>When the audit process runs, it generates the audit process result as a PDF, which is attached to the ticket that is sent to the external ticketing system. The URL to the ticket is stored in the Audit result table for external review.</p> <p>Note: Audit process results are purged following standard audit process rules. To set the purging rules, select Show advanced options from the Create New Audit Process or Details for: <audit process> page.</p>
Policy Builder for Data	<p>Policy Builder for Data uses the Alert integration point.</p> <p>Browse to Protect > Security Policies > Policy Builder for Data. Begin creating a security policy. From Rule Action, select ALERT ONCE PER SESSION or ALERT PER MATCH and then select TICKET from the Add New Action window.</p>
Risk Spotter	Browse to Protect > Uncover Threat Vectors > Active Risk Spotter. Select a user from the Risky Users table and use the Actions > Create ticket.
Threat Analytics	Browse to Protect > Uncover Threat Vectors > Active Threat Analytics. Select a case from the table and use the Actions > Create ticket.
Vulnerability Assessment Results	Browse to Harden > Vulnerability Assessment > Assessment Builder. Create and run an assessment, then click View Results. For each result that meets the test result score criteria, click Create ticket to open a ticket.

View tickets that originate from the Guardium system by opening Setup > Reports > External Tickets.

Note: Ticket status is updated every hour. Closed tickets are removed from the report after 30 days of inactivity.

Related concepts

- [Building audit processes](#)
- [Introducing Guardium Vulnerability Assessment](#)

- [Configuring the alerter](#)
 - [Certificate CLI Commands](#)
 - [Configuration and Control CLI Commands](#)
-

Configuring vulnerability scanner agents

Common Vulnerabilities and Exposures (CVE) scanner agents, such as Nessus and Qualys, gather information about the Guardium® system and send it to their third-party portal, which analyzes and generates reports. If the agent can run as root directly on the Guardium system, the resulting report is much more accurate with fewer false positive results. Use **scanner_agent** CLI commands to install and manage root access to CVE scan tools.

Before you begin

By default, vulnerability scanner agents do not have root access to the Guardium system. Without root access, the scan tools are limited to network-based scans and can detect basic information such as operating system, open ports, and cross-site scripting vulnerabilities. While a non-root scan is useful, it is limited in scope and accuracy, and as a safeguard, the network-based scans tend to result in pessimistic reports with many false-positive results. For more accurate vulnerability scan reports, allow scan tools to access the underlying Guardium system and its supporting applications and libraries (to check for CVEs) without exposing root access or creating other vulnerabilities.

About this task

Install the scanner agent on one Guardium system for each version and patch level in your environment. The scanner results for that system can represent all other systems that are at the same version and patch level. Guardium supports root access for Nessus and Qualys vulnerability scanner agents.

Procedure

1. Download a scanner agent RPM from the vendor.
 - For Guardium 11.x, the agent must support Red Hat ES 7 (x86_64).
 - For Guardium 12.x, the agent must support Red Hat ES 9 (x86_64).Example scanner agent file names:
 - Nessus - NessusAgent-10.4.2-es7.x86_64.rpm - From the Tenable Nessus Agent page.
 - Qualys - QualysCloudAgent.rpm - From the Qualys Cloud Agent page.
2. Import the scanner agent to a Guardium system by using the CLI.
For a list of supported agents, run the [`show scanner_agent_supported`](#) CLI command. The output lists the currently supported agents (`nessus` or `qualys`).
 - Import with SCP - Enter the `import scanner_agent scp <agent>` command and follow the prompts, as described in [`import scanner_agent scp <agent>`](#).
 - Import with the Guardium fileserver - Transfer the file to the fileserver, and then call the `import scanner_agent sys <agent> <filename>` command. For more information about transferring files to the Guardium fileserver, see [`fileserver`](#).
3. Configure the agent by using the [`setup scanner_agent configure <agent>`](#) CLI command and follow the prompts. The information that you need depends on the scanner agent. For more information, see [`setup scanner_agent`](#).
4. For Qualys, run `setup scanner_agent enable <agent>` to enable the agent.
Note: The Nessus agent is automatically enabled after it is configured.
5. Optional: If you use an SSL proxy, you need a certificate from a certificate authority such as DigiCert, Symantec, or Geotrust. Use the [`store_certificate scanner_ca_bundle`](#) CLI command to store the certificate. Call [`show scanner_agent ca_bundle`](#) to get the stored certificate.
Standard (non-SSL) proxies are configured with the agent in step 3.
For more information about managing certificates, see [`Certificates`](#).
6. After you install and enable the agent, it appears in the vendor's portal after a delay of up to 30 minutes.
After the agent appears in the vendor's portal, scanning and other activities are done exclusively through the portal.

Related information

- [import scanner_agent](#)
 - [restart scanner_agent](#)
 - [setup scanner_agent](#)
 - [show scanner_agent](#)
 - [start scanner_agent](#)
 - [stop scanner_agent](#)
 - [store_certificate scanner_ca_bundle](#)
 - [support must_gather_commands](#)
-

QRadar and Guardium integration

QRadar and Guardium can work together in a two-way information flow to have the Guardium data protection policies updated automatically and nearly in real-time in response to security intelligence events from QRadar.

IBM QRadar is a security intelligence tool that provides threat protection by monitoring security information and events, using customizable rules to detect anomalies, as well as providing tools for incident forensics and vulnerability management.

IBM Guardium is a solution for data security and data privacy that helps ensure the integrity of data stored in servers. Guardium uses policies and inclusion/exclusion lists (called Guardium groups) to control access to data.

The QRadar and Guardium solution leverages the QRTrigger framework for triggering actions in response to QRadar security events. Based on configuration settings, QRadar events will cause new members to be added to Guardium groups based on information carried in the event itself. Furthermore the Guardium policy associated

with the group is automatically reinstalled so that membership change takes effect immediately.

Note that the QRadar and Guardium solution can be used to update a single Guardium collector, or a group of them being controlled by a Guardium Central Manager (CM).

QRadar and Guardium together

Traditional QRadar and Guardium integration is a one-way information flow where Guardium sends alerts and Vulnerability Assessment (VA) reports to QRadar.

Common alerting use cases for databases:

- Failed logins
- Unauthorized access
- SQL Error codes (for example, SQL injection attacks)
- Users trying to escalate their privileges
- Users creating triggers and views to indirectly access sensitive data

Now QRadar and Guardium can work together in a two-way information flow.

Additional use cases:

- Block access from a machine that became compromised
- Increase audit levels for access by a user ID that became suspicious
- Increase audit levels for access by a privileged shared user ID that was on-boarded in a Privileged Identity Management (PIM) system

Updating Guardium policies based on QRadar events

The steps to deploying the QRadar and Guardium solution are:

1. Install the solution files.
2. Set up a client ID and secret in Guardium.
3. Configure a Forwarding Destination in QRadar.
4. Configure Rules to dispatch QRadar Events to the solution.
5. If necessary, define Guardium Groups and Policies for integration.

Note that Guardium version 10.1 and later has three predefined groups designed to support this integration:

- QRadarBlockingConnection
- QRadarAlertingConnection
- QRadarLogConnection

Each of these groups has the following tuple structure:

<Client IP>,<Src App>,<DB User>,<Server IP>,<Srv. Name>,<OS User>,<DB Name>

There is a predefined Guardium policy called "QRadarPolicy" with three rules: A blocking rule, an alerting rule, and a logging rule. Each rule is tied to its respective group from the list above.

Setting up Guardium

In order for the QRadar and Guardium solution to be able to authenticate to the Guardium REST API, a client ID must be registered in Guardium and the associated client secret retrieved.

Registering a client ID is done using the grdapi command line utility of Guardium. This operation is performed only once. The result of the client ID registration is a JSON entry containing details for the new client, including the client secret.

```
> grdapi register_oauth_client client_id=qrguardium
ID=0
{"client_id": "qrguardium", "client_secret": "3ac89782-ce55-
4f24-b795-b6c76ecc4045",
"grant_types": "password", "scope": "read,write", "redirect_uri":
"https://joeApp"}
ok
```

Troubleshooting logs

The QRadar and Guardium solution provides a number of log files to assist in managing and troubleshooting operations. These log files include:

Table 1. Log files

Parameter name	Description
guardiumEvents_audit.log	This an audit log of all changes made to Guardium based on QRadar events. Each line is a JSON object that includes identifiers, timestamp and details of the Event handled.
QRListener.log	Log output from the Listener process that receives forwarded event data from QRadar.

Parameter name	Description
HANDLER_<event name>.log	Log output from the dedicated handler AL for a specific Event.
RESPONSE_<event name>.log	Log output from a custom response AL if this AL implements logging based on its AssemblyLine name. For example this can be done by setting the Log Appender File Path parameter to be computed using this Javascript: return "logs/" + task.getShortName() + ".log";

OPTIM to Guardium Interface

An OPTIM to Guardium interface, using Protobuf (Universal Feed Agent), sends Optim activity logs to Guardium.

The objective of this interface is to use Guardium auditing capabilities for OPTIM activities. The auditing capabilities include: Reporting tools (user-defined queries and reports); Audit Processes (workflow automation that enables assigning a task to a role/user/group, user-defined status-flow process, escalation, export...); and, Thresholds Alerts.

The Optim-audit activity information includes the access details, session number, activity type (verb), table (object), details (fields), execution time (response time) and number of errors (records affected).

The data is mapped to the Guardium standard object model.

Enabling OPTIM auditing requires enabling via OPTIM and the steps required in Guardium are: (1) link user to Optim Audit Role; (2) add the predefined reports to the appropriate pane; (3) enable sniffer; and, (4) set policy action to Log Data With Values.

This interface includes an optim-audit role, a default layout (psml file) for the optim-audit role, and seven predefined reports.

These reports are:

- Optim - Failed Request Summary per Optim Server
- Optim - Request Execution per User
- Optim Server Optim - Table Usage Details
- Optim - Request Log
- Optim - Table Usage Summary
- Optim - Request Summary

Note: When creating the optim-audit role and user, only one tab OPTIM Audit will display. Similar to roles with custom layouts that customers can generate, this is a role layout that is meant to be used alone (the optim-audit user has no interest in the other user role tabs) but since the user role is required, layout merging has been turned off when the user has the optim-audit role so that they get only the items of optim interest. Other roles that work in this same way are "review-only" and "inv".

Note: After creating and saving the optim-audit role, click the Generate Layout selection within the User Browser menu and click Reset to get the layout associated with the role. Do this again if changing roles within the User Browser.

Combining real-time alerts and correlation analysis with SIEM products

Distribute contextual knowledge of database activity patterns, structures, and protocols directly to the third-party database of the SIEM system.

About this task

Guardium® pre-processes large volumes of database traffic and distills important information. Then, it provides the condensed summary to external SIEM (Security Incident Event Manager) systems such as ArcSight, Envision, and QRadar. Thus, SIEM products do not have to work as hard to process large traffic streams. Rather, it can concentrate on correlating all activity, alerting on unauthorized or suspicious behavior, and helping with the regulatory compliance requirements on event logs. This Guardium SIEM (Security Incident Event Manager) integration can be done in one of the following ways:

- Syslog forwarding, the most common method for alerts and events.
- Using the CLI command, **store remotelog**, to specify the Syslog forwarding to facility/priority, and host (destination). For more information, see [store remotelog](#).
- Using Guardium templates for ArcSight, Envision, and QRadar
- SCP/FTP (CSV or CEF Files sent to an external repository and the SIEM system must upload and parse from this external repository.)

Guardium distributes its contextual knowledge of database activity patterns, structures, and protocols directly to the third-party database of the SIEM system (Guardium has credentials to the SIEM system. It can also write directly to the SIEM database in the SIEM schema. Contact Guardium support as Guardium's entities must be mapped to the third-party schema.

Note: The SIEM system must enable remote logging to listen for the correct facility and priority, which is defined within syslog. For more information on configuring the facility and priority, see [Facility and priority of syslog messages](#).

By combining Guardium's real-time security alerts and correlation analysis with SIEM and log management products, companies can enhance their ability to:

- Proactively identify and mitigate risks from external attacks, trusted insiders, and compliance breaches;
- Implement automated controls from Sarbanes-Oxley (SOX), the Payment Card Industry Data Security Standard (PCI-DSS), and data privacy regulations;
- Manage system and network events alongside critical logs and events from the core of their data centers – enterprise databases and applications – for enterprise-wide correlation, forensics, incident prioritization, and reporting.

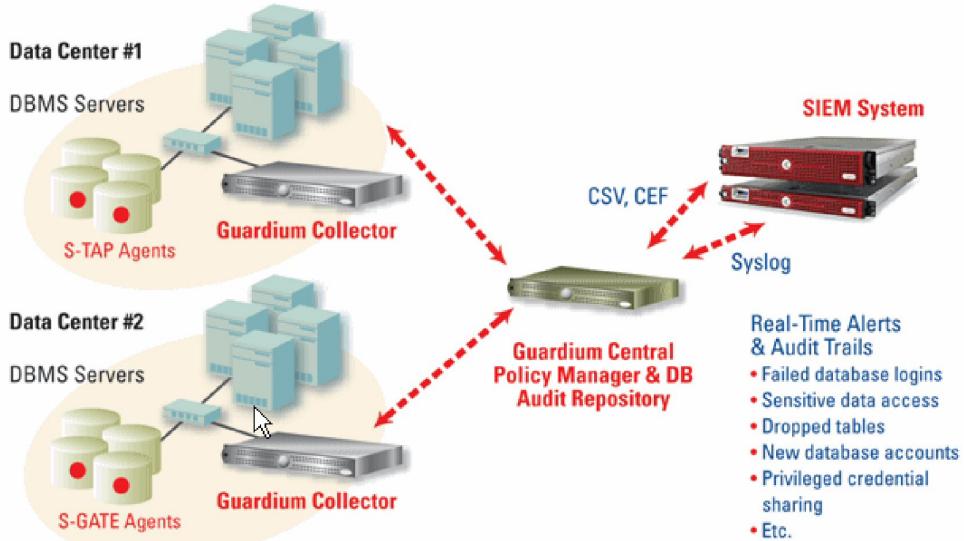
Security Information and Event Management (SIEM) solutions, also referred to as Security Event Management (SEM) solutions, are offered by companies such as QRadar, ArcSight, CA, Cisco MARS, LogLogic, RSA enVision and SenSage. SIEM products are complementary to Guardium's database activity monitoring solution. They can also use Guardium's filtering and preprocessing of database events to provide 100% visibility and database analytics for SOX, PCI-DSS, and data privacy.

SIEM technology provides real-time analysis of security alerts that are generated by network hardware and applications. It helps companies to respond to network attacks faster and to organize the massive amounts of log data that is generated daily. SIEM solutions are log-based correlation engines.

SIEM solutions are primarily focused on detection and security, but not on auditing. They assemble data from other logs and analyze it at a high level. They correlate much more data such as IP addresses and routers but have little database visibility. They do not have forensics-quality, digitally signed, audit monitoring capabilities so they can be used for immediate information, but not historical proof.

Security information and event management (SIEM) users are faced with the challenge of importing raw logs that are generated by internal DBMS utilities. The performance of DBMS logging utilities, the unfiltered information that they produce, and the lack of necessary granular information create challenges.

Through the Guardium user interface, Guardium can be configured easily to integrate with various SIEM tools.



Note: With SIEM integration, the reports and policies do not change on the Guardium system. Users can continue with their existing policies and reports, trigger alerts, and send reports to the SIEM system.

For SIEM-Guardium Integration, there are predefined templates for QRadar, Envision, and ArcSight so you do not need to define them. You can select the appropriate message template within the rule action.

You can change the default message template, specify the parameters for syslog forwarding, and create the CSV or CEF file to export.

Note: CEF is only used for ArcSight. The other SIEM products have a different format and do not use CEF.

In order for the SIEM product to recognize the information that is being sent, the message template must be changed through the Global Profile. This formatting agreement between the SIEM solution and Guardium allows SIEM products to parse incoming messages and update its own database with the new event/data.

1. To open the Global Profile, click Setup > Tools and Views > Global Profile.
2. Click Edit to Named template.

Global Profile

Use aliases in reports unless otherwise specified	<input type="checkbox"/>
PDF footer text	Copyright IBM InfoSphere
Message template	<pre>Alert based on rule ID: %ruleDescription Category: %category Classification: %classification Severity %severity Rule #: %ruleID [%ruleDescription] Request Info: [Session start: %sessionStart Server Type: %serverType Client: %clientIP (%clientHostname) Server: %serverIP (%serverHostname) Client PORT: %clientPort Server Port: %serverPort Service Name: %serviceName Net Protocol: %netProtocol DB Protocol: %DBProtocol DB Protocol Version: %DBProtocolVersion DB User: %DBUser]</pre>
No wrap	<input type="checkbox"/>
Disable accordion menus	<input type="checkbox"/>
Named template	<input type="button" value="Edit"/>

3. Select a template or create a new template with the icon.

The Guardium appliance can be configured to send Syslog messages to remote systems. Specific types of Syslog messages can be sent to specific hosts. The Syslog message type is determined from the facility-priority of the message.

Configure sending to remote systems by using the CLI command [store remotelog](#). You can test communication with the remote server using the CLI command [show remotelog_status](#). For more details on the process, see [remote syslog](#).

Examples of facility are: all, auth, authpriv, cron, daemon, ftp, kern, local0, local1, local2, local3, local4, local5, local6, local7, lpr, mail, mark, news, security, Syslog, user, uucp. Examples of priority are: alert, all, crit, debug, emerg, err, info, notice, warning.

Reports containing information that can be used by other applications or reports that contain large amounts of data can be exported to a CSV file format. Report, Entity Audit Trail, and Privacy Set task output can be exported to CSV (Delimited-separated Value) files. Additionally, CSV file output can be written to Syslog. If the remote Syslog capability is used, the output CSV file is forwarded to the remote Syslog locations.

Each record in the CSV or CEF files represents a row on the report. Contact Guardium Support for a tool that permits the reformatting of CSV files before export.

Each record in the CSV or CEF files represents a row on the report.

To send Syslog messages and export reports to CSV files, complete the following steps.

Note: Do not zip the file within the audit process definition so that the SIEM vendor can parse it correctly.

1. To open the Audit Process Finder, click Comply...> Tools and Views...> Audit Process Builder.
2. Click the  icon to add a process or select an existing process from the drop-down list.
3. Click New Audit Task under Audit Tasks.
4. Enter a description and select Report.
5. Select a report from the drop-down list and enter the CSV/CEF File Label.
6. Select Export CSV file and Write to Syslog. Choose a named template from the drop-down list.
7. Under Task Parameters, choose the Enter Period From >= and Enter Period To <= by using the calendar icon.
8. Click Apply.

CSV/CEF files can also be exported on a schedule to the SIEM host. Modify or add an audit task.

1. Click Comply...> Tools and Views...> Audit Process Builder to open the Audit Process Finder and modify or add an audit task.
2. Choose Export CSV file or Export CEF file.

Note: ACCESS reports can be saved and forwarded in CEF or LEEF format but other reports, such as Guardium Logins, Aggregation Activity Log, and CAS events cannot be mapped to CEF or LEEF.

3. Uncheck the Write to Syslog. Otherwise, Syslog messages will be generated instead of a file.
4. Open the CSV/CEF Export menu by clicking Manage...> Data Management...> Results Export (Files).
5. Select either the SCP or FTP Protocol. Then enter the Host, Directory, Username, Port, and SCP/FTP password.
6. In the Scheduling section, define the Start Time, Restart frequency, Repeat frequency, Schedule by Day/Week or Month, Schedule Start Time. Check the box to automatically run dependent jobs.
7. Click Save to commit the changes or Reset to clear the fields.

To have a policy alert that is routed to Syslog, exception rules, access rules, and extrusion rules must be modified to trigger notifications to be sent to Syslog. This action can be accomplished by going to the Policy Builder. Policy rules can be sent as email or sent to Syslog and forwarded.

1. To open the Policy Builder, click Setup...> Tools and Views...> Policy Builder.
2. Select the policy and click Edit Rule.
3. Click Add Rule...> Add Exception Rule.
4. Enter the Description, Category, Classification, and select a Severity level from the drop-down list.

For every policy rule violation logged during the reporting period, the Policy Violations report provides the Timestamp from the Policy Rule Violation entity, Access Rule Description, Client IP, Server IP, DB User Name, Full SQL String from the Policy Rule Violation entity, Severity Description, and a count of violations for that row. With this report, users can group violations and create incidents, set the severity of each violation, and assign incidents to users.

CEF Mapping

The CEF standard from ArcSight defines a set of required fields, and a set of optional fields.

The latter are called extensions in the CEF standard. Data is mapped to these fields from Guardium® configuration information and reports. Note that not all Guardium fields map to a CEF field, so there may not be a one-to-one relationship between the rows of a printed report and the CEF file produced for that report. Also note that this facility is intended to map data from data access domains (Data Access, Exceptions, and Policy Violations, for example), and not from Guardium self-monitoring domains (Aggregation/Archive, Audit Process, Guardium Logins, etc.).

Note: Analyzed Client IP has a map for CEF source. If the query used for the CEF does NOT contain the Client IP but contains the analyzed client IP, the analyzed client IP will be used for the source. If both included in the query, then Client IP takes precedence.

The CEF fields in the following table are always present.

Table 1. Required CEF fields

CEF Field	Guardium Mapping
Version	0 (zero); Currently the only version for the CEF format
Device Vendor	Guardium
Device Product	Guardium
Device Version	Guardium software version number
Signature ID	ReportID
Name	Report Title
Severity	Numeric severity code in the range 0-10, with 10 being the most important event. If not reset in the report, 0 (zero, which translates to Info for Guardium).

The CEF extension fields are optional, and will be present only when the mapping applies. For example, if the report does not contain an access rule description, the act field (the first extension field) will not be present. For more detailed information about the Guardium entities and attributes, see the appropriate entity reference topic.

Table 2. CEF extension fields

CEF Field	Entity	Attribute
severity	Policy Rule Violation	Severity
act	Policy Rule Violation	Access Rule Description
app	Client/Server	DB Protocol
app	Exception	Database Protocol
dst	Client/Server	Server IP
dst	Exception	Destination Address
dhost	Client/Server	Server Host Name

CEF Field	Entity	Attribute
dpt	Session	Server Port
dpt	Exception	Destination Port
dproc	Client/Server	Source Program
duid	Client/Server	OS User
duser	Client/Server	DB User Name
duser	Exception	User Name
end	Exception	Exception Timestamp
end	Policy Rule Violation	Timestamp
end	Access Period	Period End
end	Session	Session End
msg	Exception	Exception Description
msg	Message Text	Message Text
msg	Message Text	Message Subject
msg	SQL	SQL String
src	Client/Server	Client IP
src	Client/Server	Analyzed Client IP
src	Exception	Source Address
shost	Client/Server	Client Host Name
smac	Client/Server	Client MAC
spt	Session	Client Port
spt	Exception	Source Port
start	Exception	Exception Timestamp
start	Policy Rule Violation	Timestamp
start	Access Period	Period Start
start	Session	Session Start
proto	Client/Server	Network Protocol
request	FULL SQL	Full Sql
request	SQL	Sql
cs1	Session	Uid Chain
cs2	Session	Uid Chain Compressed

For more information about CEF, search the web for Common Event Format: Event Interoperability Standard, or visit the ArcSight Website: www.arcgis.com.

LEEF Mapping

Log Event Extended Format (LEEF) from QRadar

The LEEF format consists of an optional syslog header, an LEEF header and a collection of attributes describing the event.

Syslog_Header(optional) LEEF_Header|Event_Attributes

The LEEF header is pipe ('|') separated and attributes are tab separated

Example

Jan 18 11:07:53 host LEEF:Version|Vendor|Product|Version|EventID|Key1=Value1<tab>Key2=Value2<tab>Key3=Value3<tab>...<tab>KeyN=ValueN

Table 1. LEEF Parameters

Parameters	Description
LEEF: Version	Version Integer identifying the version of LEEF used for the log message
Vendor	String identifying the vendor of the device or application sending the event log
Product	Product String identifying product sending the event log Note: The combination of vendor and product must be unique
Version	String identifying the version of the device or application Sending the event log
EventID	ID that uniquely identifies the event
Attributes 1..N	A set of key value pairs attributes for the event separated by the tab character. Order is not enforced. A pre defined set of keys are defined and should be used when possible. LEEF format is extensible and allows for additional key value pairs to be added to the event log. Keys must not contain spaces or equal signs Values must not contain tabs

Example:

```
Jan 18 11:07:53 192.168.1.1 LEEF:1.0|QRadar|QRM|1.0|NEW_PORT_DISCOVERD|src=172.5.6.67 dst=172.50.123.1 sev=5 cat=anomaly
msg=there are spaces in this message
```

Character Encoding

UTF8

Predefined Attributes

Table 2. Predefined Attributes

Key Name	Data Type	Max Length	Description
Cat	string		Event category
devTime	date		Time the device or application emitted the event
devTimeFormat	string		Defined by the java SimpleDateFormat. This is only required if using a customized date format. See Date Format section for further details.
proto	integer		Transport protocol
sev	integer (1-10)		Severity of this event
src	IPv4 or IPv6 address		Source address
dst	IPv4 or IPv6 address		Destination address
VSrc	IPv4 or IPv6 address		Virtual source address
srcPort	integer		Source Port. The valid port numbers are between 0 and 65535.
dstPort	integer		Destination Port. The valid port numbers are between 0 and 65535.
srcPreNAT	IPv4 or IPv6 address		Source address for the message before Network Address Translation (NAT) occurred
dstPreNAT	IPv4 or IPv6 address		Destination address for the message before Network Address Translation (NAT) occurred
srcPostNat	IPv4 or IPv6 address		Source address for the message after Network Address Translation (NAT) occurred
dstPostNat	IPv4 or IPv6 address		Destination address for the message after Network Address Translation (NAT) occurred
usrName	string	255	User name associated with the event
srcMAC	MAC address		Six colon-separated hexadecimal numbers. Example: 1:2D:67:BF:1A:71
dstMAC	MAC address		Six colon-separated hexadecimal numbers. Example: 11:2D:67:BF:1A:71
srcPreNATPort	integer		Source Port. The valid port numbers are between 0 and 65535.
dstPreNATPort	integer		Destination Port. The valid port numbers are between 0 and 65535.
srcPostNATPort	integer		Source Port. The valid port numbers are between 0 and 65535.
dstPostNATPort	integer		Destination Port. The valid port numbers are between 0 and 65535.
identSRC	IPv4 or IPv6 address		
identHostName	string	255	Host name associated with the event. Typically, this parameter is only associated with identity events
identNetBios	string	255	NetBIOS name associated with the event. Typically, this parameter is only associated with identity events
identGrpName	string	255	Group name associated with the event. Typically, this parameter is only associated with identity events.

Custom Attributes

In some cases custom attributes may be required to identify more information about the event being generated. In these cases vendors may define their own custom attributes and include them in the event log. Custom attribute fields should be used only when there is no acceptable mapping in to a predefined field.

Custom attributes keys must be:

- Single word no spaces
- Alphanumeric
- Clear and concise
- Cannot be named the same as any predefined attribute key

Custom attributes may be used for viewing in the QRadar Event Viewer by creating custom properties.

Custom attributes may be used by the QRadar reporting engine by creating customer properties.

Custom attributes can NOT be used for event correlation

Note: Add databaseName=%DBname to the LEEF template in order to capture the MS-SQL database name. Update the existing LEEF template or make a new template by cloning.

Date Formats

You can use any of these predefined formats:

1. Milliseconds since January 1, 1970 (integer)
2. MMM dd yyyy HH:mm:ss, for example, Jun 06 2012 16:07:36
3. MMM dd yyyy HH:mm:ss.SSS, for example, Jun 06 2012 16:07:36.300
4. MMM dd yyyy HH:mm:ss.SSS zzz, for example, Jun 06 2012 02:07:36.300 GMT

If these formats are not suitable, you can define a custom date format in the dTime field by specifying the date format using the dTimeFormat key.

For further information on specifying a date format, visit the SimpleDateFormat page at: <http://java.sun.com/javase/6/docs/api/java/text/SimpleDateFormat.html>

Troubleshooting problems

To isolate and resolve problems with your IBM products, you can use the troubleshooting and support information. This information contains instructions for using the problem-determination resources that are provided with your IBM products, including IBM® Guardium®.

- **[Techniques for troubleshooting problems](#)**

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. Certain common techniques can help with the task of troubleshooting.

- **[Problems and solutions](#)**

Search here for solutions to problems that you encounter.

Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. Certain common techniques can help with the task of troubleshooting.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

What are the symptoms of the problem?

What is the problem? This question might seem straightforward, however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?
- Is the current environment and configuration supported?
- Do all users have the problem?
- (For multi-site installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration; many problems can be traced back to incompatible levels of software that are not intended to run together or have not been fully tested together.

When does the problem occur?

Develop a detailed timeline of events leading up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you need to look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being performed?
- Does a certain sequence of events need to happen for the problem to occur?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might have occurred around the same time, the problems are not necessarily related.

Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Consequently, problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage. If the problem is of significant business impact, you do not want it to reoccur. If possible, recreate the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

- **[Getting fixes from Fix Central](#)**

You can use Fix Central to find the fixes that are recommended by IBM Support for a variety of products, including Guardium. With Fix Central, you can search, select, order, and download fixes for your system with a choice of delivery options. A product fix might be available to resolve your problem.

- **[Contacting IBM Support](#)**

IBM Support provides assistance with product defects, answers FAQs, and helps users resolve problems with the product.

- **[Basic information for IBM Support](#)**

Before you call IBM Support, collect basic information about IBM Guardium (collector, aggregator, Central Manager; UNIX/Linux S-TAP; Windows S-TAP).

- **[Exchanging information with IBM](#)**

To diagnose or identify a problem, you might need to provide IBM Support with data and information from your system. In other cases, IBM Support might provide you with tools or utilities to use for problem determination.

Getting fixes from Fix Central

You can use Fix Central to find the fixes that are recommended by IBM Support for a variety of products, including Guardium®. With Fix Central, you can search, select, order, and download fixes for your system with a choice of delivery options. A product fix might be available to resolve your problem.

About this task

Procedure

To find and install fixes:

1. Obtain the tools that are required to get the fix. If it is not installed, obtain your product update installer. You can download the installer from [Fix Central](#).
This site provides download, installation, and configuration instructions for the update installer.
2. Select Guardium as the product, and select one or more check boxes that are relevant to the problem that you want to resolve.
3. Identify and select the fix that is required.
4. Download the fix.
 - a. Open the download document and follow the link in the Download Package section.
 - b. When downloading the file, ensure that the name of the maintenance file is not changed.
This change might be intentional, or it might be an inadvertent change that is caused by certain web browsers or download utilities.
5. Apply the fix.
 - a. Follow the instructions in the Installation Instructions section of the download document.
 - b. For more information, see the Installing fixes with the Update Installer topic in the product documentation.
6. Optional: Subscribe to receive weekly email notifications about fixes and other IBM Support updates.

Contacting IBM Support

IBM Support provides assistance with product defects, answers FAQs, and helps users resolve problems with the product.

Before you begin

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company or organization must have an active IBM *maintenance contract name*, and you must be authorized to submit problems to IBM. For information about the types of available support, see the [IBM Support Guide](#).

Procedure

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem.
For more information, see the [IBM Support Guide](#).
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
 - Online through the [IBM Support Portal](#): You can open, update, and view all of your service requests from the Service Request portlet on the Service Request page.
 - By phone: For the phone number to call in your region, see the [Directory of worldwide contacts](#) web page.

Results

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.

Basic information for IBM Support

Before you call IBM Support, collect basic information about IBM® Guardium® (collector, aggregator, Central Manager; UNIX/Linux S-TAP; Windows S-TAP).

Use **support must_gather commands**, which can be run from the CLI to generate specific information about the state of any Guardium system. This information can also be collected through the Guardium GUI.

This information can be uploaded from the Guardium system and sent to IBM Support whenever a Problem Management Report (PMR) is logged.

Encrypt Must Gather

You can configure your system to encrypt the must gather output in **Setup > Tools and Views > Global Profile..**. The default value is unencrypted, and the must gather output is compressed. When the Encrypt Must Gather output check box is checked, all future must gather output is encrypted. You can also enable encryption with the **store encrypt must_gather on** CLI command and disable it with the CLI command **store encrypt must_gather off**.

- [Running must gather in the UI](#)
Must gather collects information that Guardium support can use to help you solve issues. You can run must gather in the UI of a collector, aggregator, or central manager. You can also choose to send the results by email.
- [Running must gather from the CLI](#)
You can run **must_gather** commands from the command line interface of an IBM Guardium collector, aggregator, or central manager.
- [Running the slon looper utility](#)
The slon looper is a utility that allows Guardium to walk (loop) through your Guardium installation to gather information that can help solve customer issues. Configure and run the slon looper from the Guardium Support Information Gathering page.
- [Must gather for UNIX-Linux S-TAP](#)
You can run must gather on the collector from the UI and in the CLI, and on the database by using the **guard_diag** script.
- [Must gather for Windows S-TAP and other Windows agents](#)
Learn how to run the **diag.bat** to produce numerous statistics that help Guardium with diagnostics. Must gather has two options: S-TAP mode for S-TAPs and Standalone mode for other agents that are installed on the database server. Learn about the Pre-Kernel dump verification utility for Windows S-TAP.

Running must gather in the UI

Must gather collects information that Guardium support can use to help you solve issues. You can run must gather in the UI of a collector, aggregator, or central manager. You can also choose to send the results by email.

Procedure

1. Browse to **Manage > Maintenance > Support Information Gathering**.
2. Optional: Add a description in the text box. Enter extra information that you think Guardium support needs to know.
3. If you have a PMR or ticket number, enter it.
4. Optional: Add an email address to send the must gather files to a user. SMTP must be configured.
From **Send Results To:**, select **email:** and complete the email address. Emailed files can also be viewed in **Manage > Maintenance > Support Information Results**.
5. Optional: To start collecting log information at a future time, schedule a start time by clicking the icon.
6. Select the categories whose log information you want to include. Choose the options that most closely reflect your problems.
Note: To help troubleshoot issues for some systems, such as User Interface, Backup, and Scheduler, enter the number of minutes for the must gather to run in **Gather information duration (minutes)**. During the time period that you specify, reproduce the problem so that Guardium can generate the logs that contain the debug information. The default value is 10 minutes.
7. Click **Start** to begin running the must gather report.

Results

To view the results, browse to **Manage > Maintenance > Support Information Results**. You can open or save the **.tgz** file.

What to do next

From the Support Information Results page, you can choose how long to keep the must gather output before it is purged. The default is 30 days. To change the default, select the number of days and click **Apply**.

You can configure and run the Slon looper utility from the Support Information Gathering page. For more information, see [Running the slon looper utility](#).

Running must gather from the CLI

You can run **must_gather** commands from the command line interface of an IBM® Guardium® collector, aggregator, or central manager.

Procedure

1. Open a PuTTY session (or similar) to the appropriate collector, aggregator, or central manager.
2. Log in as user `cli`.
3. Depending on the type of issue, enter the relevant `must_gather` commands into the CLI prompt in the format `support must_gather <issue>`. You might need more than one of the following `must_gather` commands to diagnose the problem.
 - `agg_issues` - Aggregation process issues.
 - `alert_issues` - Alerting issues.
 - `app_issues` - Application issues.
 - `audit_issues` - Audit process issues.
 - `auth_issues` - Authentication issues (including LDAP and multifactor authentication).
 - `auto_create_ie` - Auto create inspection engines issues.
 - `backup_issues` - Backup process issues.
 - `big_data_issues` - Big data issues.
 - `cm_issues` - Central manager issues.
 - `compliance_mon_issues` - Compliance monitoring issues.
 - `datamining_issues` - Data mining issues.
 - `datastreams_issues` - Data streaming issues.
 - `deploy_agents_issues` - Deployment agents issues.
 - `deployment_issues` - Deployment issues.
 - `eagle_eye_issues` - Advanced threat scanning issues.
 - `enterprise_load_balancer_issues` - Enterprise load balancer issues.
 - `entitlement_issues` - Entitlement optimization issues.
 - `go_stream` - Go stream issues.
 - `jproxy_issues` - Jproxy issues.
 - `miss_dbuser_prog_issues` - System database user issues.
 - `native_auditing_issues` - Native auditing issues.
 - `network_issues` - Network architecture issues.
 - `patch_install_issues` - Patch installation and upgrade issues.
 - `purge_issues` - Purge process issues.
 - `risk_spotter` - Risk spotter issues.
 - `scanner_agent_issue`
 - `scheduler_issues` - Scheduler issues.
 - `slon_looper` - Slon looper output.
 - `sniffer_issues` - Sniffer issues.
 - `system_db_info` - Guardium system database or operating space performance issues.
 - `universal_connector_issues` - Universal connector issues.
4. Generate and send the resulting output to IBM Support:
 - Running the `must_gather` can take several minutes. When complete, you can retrieve the file with the `fileserver` command. For more information, see [fileserver](#). On the fileserver, the `must_gather` files are stored in the `..//Access logs//opt-ibm-guardium-log/**/must_gather/` directory. Within the directory, Guardium generates the logs as `.tgz` files.
 - Upload any `must_gather` files to ECUREP by using standard data upload. Specify the PMR number and the file to upload.

Running the slon looper utility

The slon looper is a utility that allows Guardium to walk (loop) through your Guardium installation to gather information that can help solve customer issues. Configure and run the slon looper from the Guardium Support Information Gathering page.

About this task

The slon looper logs message dumps and MustGather information that Guardium technical support can use to help reproduce and resolve customer issues. The slon looper saves a message dump when the conditions that you specify are found in the customer's environment, such as incorrect database usernames or missing session parameters. After these conditions are satisfied, the looper saves the MustGather data alongside the message dump. Guardium technical support can replay the message dumps in IBM's secure environment to reproduce the issue. Typically, message dumps are extensive binary files. In specific scenarios, especially with firewall and query rewrite issues, the looper might log an encrypted text SLON file, as a message dump might not provide the needed insights. Work with Guardium technical support to determine how to configure the slon looper for your needs.

Procedure

1. Browse to `Manage > Maintenance > Support Information Gathering`.
2. Follow the instructions in [Running must_gather in the UI](#), and select Slon looper. Do not select any other categories. Looper configuration displays.
3. Click Select to open the Select looper configuration window.
 - If one or more slon looper configurations are available, select a looper and click Save.
 - If you do not have an existing configuration, click  to open the New looper configuration window. For more information about configuring an slon looper, see [Configuring the slon looper utility](#).
4. After you select an slon looper configuration, click Start to begin running the slon looper.

Results

To view the results, browse to `Manage > Maintenance > Support Information Results`. You can open or save the `.tgz` file.

What to do next

If you need detailed login information to solve your issue, Guardium technical support might suggest that you configure and run the `Login information dump` session level policy. For more information, see [Session-level policies](#) and [Login information dump example](#).

- [Configuring the slon looper utility](#)

Before you can run an slon looper, you need to configure one from the Support Information Gathering page. Use the slon looper to investigate an incoming network traffic problem on the sniffer.

Configuring the slon looper utility

Before you can run an slon looper, you need to configure one from the Support Information Gathering page. Use the slon looper to investigate an incoming network traffic problem on the sniffer.

The slon looper utility allows you to create a looper configuration from Guardium sniffer data. You can create a general slon looper that looks for either specific traffic patterns or searches for information in log files.

Configuring a general slon looper

1. Open the New looper configuration window, as described [Running the slon looper utility](#).
2. Enter a meaningful name for this looper utility.
3. Select the Issue type that reflects your issue. If you don't know, select Other. Depending on the issue type that you select, Guardium sets other parameters. In this case, use the specified defaults.
4. Select Looper options:
In most cases, you can use the defaults. Work with Guardium technical support to determine whether you should make changes to these options.
 - Collect msg-dump - Selected by default.
 - Collect slon file - This file is useful when you need to investigate issues related to the firewall, query rewrite, timing issues, or session level policies.
 - Collect snif must_gather - Selected by default. The slon looper utility analyzes the sniffer log output to help determine sniffer issues.
5. Set the options for running the slon looper:
 - Number of loops - The count of message dumps and "must gather" data instances where conditions for logging (as defined in the looper) are met.
 - Loop duration - The maximum time allotted for looper logging. If the specified conditions aren't met within this period, the slon looper discards the existing message dump and starts again.
 - Looper timeout - The maximum length of time that a looper can run if its conditions aren't met.
 - Max file size - The maximum size of the logged message dump to ensure the server's disk space isn't exhausted.
6. Optionally select an additional filter:
 - a. Select Traffic filters and then select one of the filters from the list.
 - b. Select or enter the information for that filter.
For example, if you select Server IP address, then select an operand and enter an IP address (or use regex to find a range of IP addresses).
7. When you are done, click Save and then click Save again to select the slon looper configuration that you created and return to the Support Information Gathering page.
8. Click Start to run the slon looper utility. You can view the output from the Support Information Results page, as described in [Running the slon looper utility](#).

Or

- a. Select Log files search.
- b. Specify a search string for either the syslog or the sniffer log.

Configuring a custom slon looper

If you work with Guardium technical support on a sniffer issue, your support team might send you an ad hoc sniffer patch to debug an issue or test a fix.

Click Custom and then follow the instructions from your support team to upload and run the ad hoc patch.

Must gather for UNIX-Linux S-TAP

You can run must gather on the collector from the UI and in the CLI, and on the database by using the guard_diag script.

You can run must gather by either of these methods.

- In the S-TAP Control page: Under the specific S-TAP, click . In the S-TAP Commands window, select the command STAP logging, check Run Diagnostics, then click Apply. The logs will get uploaded to the Support Information Gathering Results page.
- Log in to the database server. The location of the diagnostics script (guard_diag) depends on the installation method.
 - Shell: The directory you specified during the S-TAP installation. By default, /usr/local/guardium/guard_stap
 - GIM: /usr/local/guardium/modules/STAP/current/guard_diag
 - .rpm: /opt/guardium/guard_stap/guard_diag. This is hard coded, and cannot be changed.

The script prompts for the location if the script cannot automatically determine where S-TAP is installed. The run time is a few minutes. If no output directory is specified, the script saves the generated .tar file in /tmp. When the script runs and enables logging from the GUI, the .tar file is placed in /var/tmp. The file name is derived from the server name, and the time and date it ran. It always starts with diag.ustap.

The verbosity of the output is set by the diagnostics, and does not need modification.

By default, diagnostics are uploaded to the Support Information Gathering Results page in the collector. The upload is controlled by the guard_tap.ini parameter upload_feature. The default value is 1. For more information, see [upload feature](#).

The S-TAP log file records the successful transfer of a diagnostics .tar file to the appliance. It also records a failure message if the .tar file is not sent to the appliance, with debug details on the failure.

General system data collected:

- Uname -a
- List of kernel modules installed
- Output for one cycle
- Uptime
- Processor number and type
- Dump of most recent syslog
- Netstat output
- IPC list
- Disk free statistics
- Copy of /etc/services
- Directory listing of /etc
- Various platform-specific information
- Contents of /etc/inittab

S-TAP Data collected:

- S-TAP version
- Contents of guard_tap.ini
- Ls -l on the K-TAP device nodes
- A-TAP diagnostics (output of the atap_must_gather.sh) (see [S-TAP is not capturing A-TAP traffic](#))
- All Exit diagnostics (for Db2, this is the output of the db2_exit_health_check.sh. See also [Linux S-TAP is not capturing Db2 exit traffic](#).)
- 30s trace of S-TAP
- K-TAP statistics
- List of all the files in the installation directory
- Verbose debug log for K-TAP (2) and S-TAP (4)
- Database configuration information: Either files, or output from a database command, depending on the database type. For example, Oracle: listener.ora, sqlnet.ora, and tnsnames.ora; Informix: onconfig.* and sqlhosts.*"; Sybase: interfaces and *.cfg; Db2: output of Db2 command: **db2 get dbm cfg**

Limitations:

- Tusc is not installed on all HP-UX operating systems, so tracing the S-TAP PID does not work.
- gzip isn't always installed on the system. The fallback is to compress (final extension of .tar.Z) and failing that, the .tar file is placed in the output directory.
- Topas output on AIX is best interpreted by the terminal since it contains control codes that make it mostly unintelligible when it is opened in an editor.
- The non-root S-TAP has a number of issues related to the diagnostics script.
- In Linux, /var/log/messages is only readable by the root.
- Some Solaris operating systems might not be configured correctly, which causes netstat to print an error.
- The path for the non-root user is rather basic, and as a result, some commands might not run at all. Notably, this known issue happens on HP-UX with gzip.
- Platform-specific requirements:
 - S-TAP: None
 - Linux: None
 - AIX: topas
 - Solaris: top, prtdiag, psrinfo

Supported platforms:

- Linux
- HP-UX
- AIX
- Solaris

Must gather for Windows S-TAP and other Windows agents

Learn how to run the diag.bat to produce numerous statistics that help Guardium with diagnostics. Must gather has two options: S-TAP mode for S-TAPs and Standalone mode for other agents that are installed on the database server. Learn about the Pre-Kernel dump verification utility for Windows S-TAP.

S-TAP mode

Run diag.bat with any of:

- Log in to the database server. From the Windows Start menu, go to IBM Windows S-TAP > Run Diagnostics.
- Log in to the database server. Open the Windows Command Prompt as Administrator. Change the directory to %WINSTAP_DIR%\bin (for example C:\Program Files\IBM\Windows S-TAP\bin). Run diag.bat
- In the S-TAP Control page: Under the specific S-TAP, click . In the S-TAP Commands window, select the command STAP logging, check Run Diagnostics, then click Apply. The logs are listed in the Support Information Gathering Results.

When you run diag.bat as a command prompt, it has a number of **command options**: **diag.bat [h] [v] [s] [k]**

You can specify only one option each time you run the command. For example:

diag.bat h

or

diag.bat help

Command option	Description
h, help	Display help
v, version	Display the version.

Command option	Description
s, summary	Create a summary of important information from several files, such as system.txt and guard_tap.ini and generates a file called summary.txt. This summary file contains the most useful information that you need. Running summary can take a few minutes.
k, keep	Keep all files in the ZIP_SOURCE_DIR after the files are zipped. This is useful if you want to review the files on database DB server without unzipping the zip file. If this option is not specified, all files copied from Guardium folders are removed from the diag folder after the zip is created. <ul style="list-style-type: none"> • ZIP_SOURCE_DIR for S-TAP: %WINSTAP%\Logs • ZIP_SOURCE_DIR for standalone: ~\diag

The output of diag.bat is a compressed file. You can access it:

- In the folder %WINSTAP%\bin\zipTmp on the DB server with a name in the format WSTAP_HOST_YYYY-MM-DDTHH-MM-SSTZD.zip.
- From the Guardium Support Information Gathering Results page.

The compressed file contains numerous files in a few sections:

- root directory of the compressed file: driver logs and environmental details
- install: Installer logs
- diag: environment details and must gather
- ini: guard_tap.ini

These folders display when the product is installed in the database server:

- Windows S-TAP (when root folder is in S-TAP mode): S-TAP configuration and log files
- Guardium Installation Manager: GIM configuration and log files
- Guardium Agent Monitor: GAM configuration and log files
- Windows Fam Monitor: FAM configuration and log files
- CAS: CAS configuration and log files
- FAMCrawler
- FAMforSP
- FAMforNAS
- FDECforNAS
- FDECforSP

When you run **diag.bat**, it creates a log of the process: diag.log. The log files contain the log level (Information, Warning, Error), timestamp, and details of activities. This log can help you if **diag.bat** did not run successfully. It is included in the diagnostics file.

Standalone Must Gather

In Standalone mode you can run the Must Gather (diag.bat) script for any installed Guardium Windows agent: GIM, GAM, FAM monitor, FDEC for SP, FDEC for NAS, FAM for SP, FAM for NAS. You can run it from any folder, for example, C:\tmp.

To run diag.bat, open the Windows Command Prompt as Administrator, and run diag.bat. The output compressed file is generated in %PRODUCT_DIR%\Bin\zip\GRD_WIN_xxxx.zip. The format of the compressed file name is GRD_WIN_%YYYY-MM-DD%T%HH-MM-SS-msec%%TZD%, where TZD is time zone difference. One compressed file is kept in the folder. Older compressed files are deleted automatically.

The Upload feature (controlled by the S-TAP parameter UPLOAD_FEATURE) does not support Standalone must gather.

The directory structure of the standalone must gather is:

- The environment details are in the root directory of the compressed file.
- Driver logs, ini, are under the Windows S-TAP folder.
- Others are the same

If you run **diag.bat** but do not get results, and a warning message displays in ~\zip\GRD_WIN_DIAG_compress-archive_failed.txt, the powershell version is lower than V5.1. You can access the files under the \diag directory. If you can install Windows Management Framework (WMF) V5.1, then **diag.bat** can create the compressed file.

Tip: You can use the standalone mode to troubleshoot failed installations of Windows agents. For example, a Windows GIM installation failed, and nothing is copied to the database server. Copy **diag.bat** V2.1 from the Win GIM V11.3 installer and put it anywhere on the database server (for example C:\work\diag.bat). Open the Windows Command Prompt as Administrator and run C:\work\diag.bat. This gathers the OS information, install logs, and other Guardium logs if they exist.

Table 1. Difference between the modes

	S-Tap Mode	STANDALONE Mode
Location of diag.bat	%WINSTAP_DIR%\bin\diag.bat	Anywhere except Win S-TAP dir
Location of diag.log	%WINSTAP_DIR%\bin\diag\diag.bat	~\diag\diag.log
ZIP source folder	%WINSTAP_DIR%\Logs	~\diag
ZIP target folder	%WINSTAP_DIR%\bin\zipTmp	~\zip
ZIP file name	WSTAP_%HOST%_%YYYY-MM-DDTHH-MM-SSTZD%.zip	GRD_WIN_DIAG_%YYYY-MM-DDTHH-MM-SSTZD%.zip
ZIP tool	ExternalZip.exe	Powershell compress-archive command
Command Options	Supported	Supported
S-TAP features (Run from GUI/ upload)	Supported	NOT Supported

Pre-Kernel dump verification utility for Windows S-TAP

Run this utility before run a kernel dump to ensure that the dump can be created without problems.

Run the utility, SystemVerificationTool.exe, from its location in the S-TAP installed directory.

A window opens with the status, the configured dump type, the CPU size, and the free disk space. If the configuration is good for a kernel dump, the status is The system is correctly configured for a kernel dump. If the configuration is not good for a kernel dump, it informs you why.

Message	What to do
Dump type is not configured as kernel type.	Click the link and follow the procedure to change the dump type, then run the utility again.
There is only one CPU, generating a dump may lock up the CPU.	Kernel dump is not recommended
Disk space is too low to handle the creation of the dump, generating a dump may lock up the CPU.	Free up disk space and run the utility again. The utility requires the smaller of: one third of physical memory, or 10 GB.

- [Running Must Gather V3.0](#)

Running Must Gather V3.0

Listed are a few different methods to run Must Gather V3.0

Method 1. Run Must Gather V3.0 from the GUI

- Login to the Guardium GUI and navigate to the S-TAP Control tab.
- Click the Send Command icon on the target S-TAP Host.
- Select STAP Logging from the drop down menu next to Command.
- Check the Run Diagnostics check box and then press the Apply button.

Note: It may take several minutes or more for this process to complete. The diagnostic files will be archived to a zip file and uploaded to the collector. You can access this information from the Guardium GUI. Login to the Guardium GUI navigate to the Manage section, underneath locate Maintenance, and then click Support Information Results.

Method 2. Run Must Gather from Windows Start Menu

- Login to the DB server where the Windows S-TAP is installed.
- Navigate to the Windows Start menu, then navigate to the IBM Windows S-TAP folder open it and choose the Run Diagnostics application.

Note: The elevated Windows Command Prompt will then open up and the Must Gather script will start. The diagnostic files will be archived and stored to %WINSTAP_DIR%\Bin\zipTmp*.zip . It will also be sent to the collector if the upload feature is enabled in Windows S-TAP.

Method 3. Run Must Gather from Windows Explorer

- Login to the DB server.
- Right click the diag.bat file and choose Run as Administrator.

Note: If you run diag.bat which is under %WINSTAP_DIR%\Bin , it'll run as S-TAP mode and the diagnostic files will be archived and stored to %WINSTAP_DIR%\Bin\zipTmp*.zip. If you run diag.bat which is NOT under %WINSTAP_DIR%\Bin, it'll run as STANDALONE mode and the diagnostic files will be archived and stored to %current_dir%\zip*.zip.

Method 4. Run Must Gather from Windows Command Prompt as the Administrator

- Open Windows Command Prompt as the administrator
- Change the directory to the location where the diag.bat and diag.ps1 files are located.
- Run diag.bat.

Method 5. Run Must Gather Power Shell script (diag.ps1) directly

Must Gather V3.0 is written in Power Shell so you can run diag.ps1 directly without have to use the diag.bat file.

Example 1: Open Windows Command Prompt as the administrator and run powershell ./diag.ps1 on the directory where diag.ps1 is located.

Example 2: Open PowerShell as the administrator and run ./diag.ps1 on the directory where diag.ps1 is located.

Exchanging information with IBM

To diagnose or identify a problem, you might need to provide IBM Support with data and information from your system. In other cases, IBM Support might provide you with tools or utilities to use for problem determination.

Sending information to IBM Support

To reduce the time that is required to resolve your problem, you can send trace and diagnostic information to IBM Support.

Procedure

To submit diagnostic information to IBM Support:

1. Open a problem management record (PMR).
2. Collect the diagnostic data that you need. Diagnostic data helps reduce the time that it takes to resolve your PMR. You can collect the diagnostic data manually or automatically:
 - Collect the data manually.
 - Collect the data automatically.
3. Compress the files by using the .zip or .tar file format.
4. Transfer the files to IBM.

You can use one of the following methods to transfer the files to IBM:

- [The Service Request tool](#)
- Standard data upload methods: FTP, HTTP
- Secure data upload methods: FTPS, SFTP, HTTPS
- Email

Receiving information from IBM Support

Occasionally an IBM technical-support representative might ask you to download diagnostic tools or other files. You can use FTP to download these files.

Before you begin

Ensure that your IBM technical-support representative provided you with the preferred server to use for downloading the files and the exact directory and file names to access.

Procedure

To download files from IBM Support:

1. Use FTP to connect to the site that your IBM technical-support representative provided and log in as anonymous. Use your email address as the password.
2. Change to the appropriate directory:
 - a. Change to the /fromibm directory.

```
cd fromibm
```

- b. Change to the directory that your IBM technical-support representative provided.

```
cd nameofdirectory
```

3. Enable binary mode for your session.

```
binary
```

4. Use the **get** command to download the file that your IBM technical-support representative specified.

```
get filename.extension
```

5. End your FTP session.

```
quit
```

Problems and solutions

Search here for solutions to problems that you encounter.

- [**User interface**](#)
These sections present troubleshooting and solutions for common user interface problems.
- [**Troubleshooting Guardium Data Protection policies**](#)
These sections present troubleshooting and solutions for common user interface problems.
- [**Troubleshooting Guardium Data Protection reports**](#)
These sections present troubleshooting and solutions for common problems with reports.
- [**Troubleshooting Guardium Data Protection issues with assessing and hardening an environment**](#)
These sections present troubleshooting and solutions for common problems with assessing and hardening.
- [**Troubleshooting Guardium Data Protection configuration**](#)
These sections present troubleshooting and solutions for common problems with configuring your Guardium system.
- [**Access management**](#)
These sections present troubleshooting and solutions for common problems with access management.
- [**Aggregation**](#)
These sections present troubleshooting and solutions for common problems with aggregation.
- [**Internal database**](#)
These sections present troubleshooting and solutions for common problems with the internal database.
- [**Central management**](#)
These sections present troubleshooting and solutions for common problems with central management.
- [**S-TAPs and other agents**](#)
These sections present troubleshooting and solutions for common problems with S-TAPs and other agents.
- [**Collectors**](#)
These sections present troubleshooting and solutions for common problems with collectors.
- [**Troubleshooting Guardium Installation Manager \(GIM\)**](#)
These sections present troubleshooting and solutions for common problems with GIM.
- [**File activity**](#)
These sections present troubleshooting and solutions for common problems with file activity and classification.
- [**Investigation dashboard**](#)
These sections present troubleshooting and solutions for common problems with the investigation dashboard.
- [**Troubleshooting Guardium Data Protection installation**](#)
These sections present troubleshooting and solutions for common problems encountered when installing your Guardium system.
- [**z/OS**](#)
These sections present troubleshooting and solutions for common problems with z/OS.

User interface

These sections present troubleshooting and solutions for common user interface problems.

- [**Changes are not saved when you add an inspection engine**](#)
If your changes are not saved when you add an inspection engine, check that the parameters are valid.
- [**HTTP error 403**](#)
If you receive a HTTP error 403, you can disable the Cross-Site Request Forgery (CSRF) protection feature to prevent the error.

- **Java.lang.IllegalStateException**
If you receive a java.lang.IllegalStateException error, clean up the Java servlets.
- **Pages are not loading correctly**
If pages do not load correctly, restart the GUI or use a different browser.

Changes are not saved when you add an inspection engine

If your changes are not saved when you add an inspection engine, check that the parameters are valid.

Symptoms

When you add an inspection engine, the new settings remain for a few minutes and then disappear.

Causes

There is an error in one or more parameter values with either the new inspection engine or a different inspection engine in the S-TAP configuration file guard_tap.ini.

Environment

The Guardium collector user interface is affected.

Resolving the problem

Check that every parameter that must be set for the inspection engine is set to a valid value. For example, some database types require that you set db_install_dir to the path of the installation directory on the server. However, for other database types, this parameter must not be set or must be set to NULL. Check the specific requirements for your database type in the S-TAP Help Book and make sure that everything is correctly set.

HTTP error 403

If you receive a HTTP error 403, you can disable the Cross-Site Request Forgery (CSRF) protection feature to prevent the error.

Symptoms

When you refresh the IBM® Guardium® GUI from the system main page, you receive the following error:

```
HTTP Status 403-
type Status report
message
description Access to the specified resource () has been forbidden
```

Causes

The cause is a feature in Guardium designed to prevent Cross-Site Request Forgery (CSRF). CSRF protection is enabled by default.

Environment

All Guardium configurations (collector, aggregator, central manager) are affected.

Resolving the problem

You can disable this feature by using the following CLI command: **store gui csrf_status off**

Note: If you turn off CSRF protection, the security level of the Guardium system is reduced.

The following command enables protection against Cross-Site Request Forgery. It is enabled by default: **store gui csrf_status on**

You can check the status by running this CLI command: **show gui csrf_status**

Java.lang.IllegalStateException

If you receive a java.lang.IllegalStateException error, clean up the Java servlets.

Symptoms

You receive the following error message.

```
There has been an Error. Please Contact your System Administrator
(java.lang.IllegalStateException)
```

Causes

The error is raised when a method is invoked and the Java VM is in a state that is inconsistent with the method. There might also be corrupted Java servlets that are caused by deadlocks.

Environment

The Guardium system is affected.

Resolving the problem

Wait a few minutes and retry. If the error persists, restart the GUI by logging in as user cli and executing the command **restart GUI**.

To clean up the Java servlets, run the command **support clean servlets**.

If the problem is not resolved, please collect the following tomcat logs and contact IBM® Guardium® Technical Support.

`tomcat_log/localhost.<date_stamp>.log`
`tomcat_log/catalina.<date_stamp>.log`

Pages are not loading correctly

If pages do not load correctly, restart the GUI or use a different browser.

Symptoms

You might see a blank screen or other errors. The problem appears to happen with certain browsers on specific systems but not with others.

Causes

The cause might be restricted to a localized browser or there is a Java virtual machine issue.

Environment

The collector, aggregator, and central manager are affected.

Resolving the problem

To resolve the problem, run **restart GUI** from the CLI prompt on the Guardium system. If that does not help, try the following actions.

- Restart the system.
 - Uninstall and reinstall the Java virtual machine.
 - Uninstall and reinstall the browser.
 - Use a different browser.
-

Troubleshooting Guardium® Data Protection policies

These sections present troubleshooting and solutions for common user interface problems.

- [Query does not appear in the co-relation alert definition](#)
If the query does not appear in the co-relation alert definition, check the count field and sort by time stamp.
 - [Rule does not trigger](#)
If a rule with a value in the policy command field does not trigger as expected, reconfigure the rule.
 - [REDACT function causes overly masked result](#)
There can be several reasons why the REDACT function causes an overly masked result. Some possible ways to resolve your issue are provided here.
 - [REDACT - Working with regex on Windows DB servers](#)
When you use regular expressions with REDACT with Windows database servers, you need to be aware of some caveats and workarounds.
 - [SSH sessions and automated CRON jobs that log in to your Oracle database are shown as failed logins](#)
If SSH sessions and automated CRON jobs that log in to your Oracle database are shown as failed logins, amend the policy.
-

Query does not appear in the co-relation alert definition

If the query does not appear in the co-relation alert definition, check the count field and sort by time stamp.

Symptoms

You created an access query for creating a co-relation alert. However, in the co-relation alert definition, this query does not appear in the drop-down list.

Causes

The co-relation alert search in the report is based on the time stamp.

Environment

The collector and aggregator are affected.

Resolving the problem

Mark the Add Count check box and sort by time stamp.

Rule does not trigger

If a rule with a value in the policy command field does not trigger as expected, reconfigure the rule.

Symptoms

Rules with a value in the policy Command field do not trigger as expected.

Causes

The cause is a misconfiguration in the command field. The Guardium parser does not consider the command modifiers to be a part of a command.

Environment

Guardium Collectors. The command field in the policy rule is also affected when it is used with wildcard (%).

Resolving the problem

The value in the Command field of the rule must match a value exactly that is shown in SQL Verb, plus a wildcard (%) as needed. This example is correct.

```
GRANT  
GRANT%
```

This example is incorrect.

```
GRANT% TO PUBLIC  
%GRANT% ADMIN OPTION%
```

ADMIN OPTION and **TO PUBLIC** do not match and cannot trigger a rule because the Guardium parser does not recognize them as a part of a command. Generally, the parser does not consider command modifiers to be part of a command. Instead, create a report to inspect the traffic that the policy monitors and include the SQL Verb field from the Command entity in that report. Anything that is listed in the SQL Verb field is recognized by the parser and can be used in the Command field of a policy rule. Several commands can be added to a group and the group can be used in the rule instead of a single command. In this case, each group member must match an entry in SQL Verb. Guardium includes several such command groups that you can use or clone.

REDACT function causes overly masked result

There can be several reasons why the REDACT function causes an overly masked result. Some possible ways to resolve your issue are provided here.

Symptoms

The redact function causes an overly masked result or an ORA-03106 error in Oracle traffic.

Causes

The redact function in the Guardium policy rule is doing a pattern match with the result set. It has a feature to replace the matched string with the user specified character.

Environment

Guardium collectors are affected.

Resolving the problem

Use the regular expression `\x0c{1}[0-9]{8}([0-9]{4})`. This regular expression ensures that it starts with the length of the column followed by 12 digits and replaces the last 4 digits.

For Windows databases:

- For Microsoft SQL with VARCHAR only, you must specify the exact number (from 01 to 99) of characters to redact. Specify the number in angle brackets. For example, to redact the first 10 characters of your string:

```
<10>([0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]
```

- For Microsoft SQL, you can also use the following expression to redact the first 6 digits of a 10-digit number:

```
[\x0A\x14]([0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]
```

Where |x0A represents 10 bytes and |x14 represents 20 bytes.

Note: For more information about using regex with Windows, see [REDACT - Working with regex on Windows DB servers](#).

REDACT - Working with regex on Windows DB servers

When you use regular expressions with REDACT with Windows database servers, you need to be aware of some caveats and workarounds.

Symptoms

When you use Guardium® REDACT in your policy, the policy does not recognize the following regular expressions:

Regex	Description
{n}	Repeat n times. That is, match the preceding item n times.
/xNN	2-digit hex number. Use / xNN instead (with backslash).
/NNN	3-digit octal number. If possible, specify the ASCII equivalent.

Causes

Windows server does not support all regular expression patterns.

Note: REDACT policies that use regex can only scrub null-terminated data types.

Environment

Guardium collectors that receive data from Windows database servers.

Resolving the problem

Depending on the regex issue, rewrite your regex as follows:

- Instead of {n}, specify each digit that you want to match. For example, instead of the following regex:

```
[0-9]{5}
```

Use the following expression:

```
[0-9][0-9][0-9][0-9][0-9]
```

- Use /|xNN| to signify a 2-digit hexadecimal number, such as /x41/.

Where /|xNN| is a hexadecimal number between 01 to FF (|x00 is not supported).

For example, the hexadecimal number x41 maps to the ASCII character A. In this case, you can use either of the following regular expressions to add the letter A to the beginning of any 4-digit number:

```
[\x41][0-9][0-9][0-9][0-9]
```

Or:

```
A[0-9][0-9][0-9][0-9]
```

To use /|xNN| for redaction, specify the length of the entire string as a 2-digit hexadecimal number, and then wrap the characters to redact in parentheses.

Note: For Microsoft SQL, each character is two bytes. For most other data sources, each character is one byte.

For example, to redact the first 6 digits of a 10-digit number, use the following regex:

For MS SQL data sources:

```
\x14([0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]
```

For other (non-MS SQL) data sources:

```
\x0A([0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]
```

To make sure that your regex works with most data sources, use the following regex:

```
[\x0A\x14]([0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]
```

Where, the /|x0A|x14/ part of the pattern means either-or. The redaction engine first tries the |x0A pattern, and if that doesn't match, it tries the |x14 pattern.

Note: For Microsoft SQL with VARCHAR only, you must specify the exact number (from 01 to 99) of characters to redact. Specify the number in angle brackets. For example, to redact the first 10 characters of your string:

```
<10>([0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9][0-9]
```

- /|NNN| signifies a 3-digit octal number such as 102. Windows S-TAP does not support this pattern.

No perfect alternative pattern exists, but if [NNN] matches to a specific ASCII character, you can replace the octal number with its ASCII counterpart. For example, the octal number 102 maps to the ASCII character B. In this case, you can replace the following regex:

```
[102] [0-9] [0-9] [0-9] [0-9] [0-9]
```

With this expression:

```
B [0-9] [0-9] [0-9] [0-9] [0-9]
```

If one of these patterns does not resolve the problem in your environment, contact IBM® Technical Support if you need further analysis.

SSH sessions and automated CRON jobs that log in to your Oracle database are shown as failed logins

If SSH sessions and automated CRON jobs that log in to your Oracle database are shown as failed logins, amend the policy.

Symptoms

SSH sessions and automated CRON jobs that log in to your Oracle database through SQLPLUS and RMAN with /as sysdba show as failed logins.

Causes

Oracle responds to these logins with the following error on such attempts, even if it is not shown on the screen.

```
ORA-01-17: invalid username/password; logon denied.
```

This error triggers the failed login alert. For example, if the database user WRONGLOGIN is a member of the DBA group, and logs as sqlplus WRONGLOGIN as sysdba, the database authentication of WRONGLOGIN fails. This failure causes the ORA-01-17 error alert to trigger and is reflected in the Guardium log. However, users with sysdba privileges can connect to the database without database authentication so the session is allowed to continue. Both events are captured and recorded.

Environment

Guardium collectors are affected.

Resolving the problem

You can amend the policy to include an allow action before the rule that alerts about failed logins. Create an exception rule in the policy with the following conditions.

```
Client IP=<Server IP>
Source program = SQLPLUS
DB user in trusted group
OS user in group of Oracle DBAs
Net protocol = BEQUEATH (if local BEQUEATH, not TCP)
```

This rule skips the failed login alerts that are caused by the ORA-01-17 error but are still logged. To filter the failed login alerts out of the reports, add these conditions to the end of the conditions list:

```
AND
(
    client IP<>server IP OR
    src prg <> SQLPLUS OR
    db user NOT IN group of trusted OR
    os user NOT IN group of oracle DBAs OR
    net protocol <>BEQUEATH (if this is local BEQUEATH, not TCP )
)
```

Troubleshooting Guardium® Data Protection reports

These sections present troubleshooting and solutions for common problems with reports.

- [Cannot modify the receiver table for an Audit Process after it has been executed at least once](#)
If you cannot modify the receiver table for an audit process, clone the audit process and replace the original.
- [Cannot see multi-byte characters](#)
If you export a Guardium report to PDF and the characters are not correct, switch the PDF font configuration.
- [File system is almost full](#)
If the Guardium file system is almost full, change the log rotation strategy.
- [Guardium audit reports viewed in Microsoft Excel have rows with unexpected characters](#)
If you view an Audit report in .csv and see rows with unexpected characters, use another .csv viewer or view it as a .pdf file.
- [Reports show IP address as 0.0.0.0](#)
- [Request was interrupted or quota exceeded error message](#)
If you receive an error message that states the request was interrupted or the quota was exceeded when you run a report, divide the report into pieces of shorter reporting interval.
- [Scheduled Job Exceptions every 5 minutes](#)
If you receive a Scheduled Job exception every 5 minutes, deactivate the alert from the Anomaly Detection page.

- [Scheduled jobs exception: merge required, delay executing process](#)
If you receive an error message that states merge required, delay executing process, reschedule the Audit process.
- [The database user is not shown correctly in Guardium reports when you monitor Teradata](#)
If Guardium reports do not show the database user correctly when you monitor Teradata, configure the Teradata Database.
- [Unexpected results in Guardium reports with embedded commands](#)
If you receive unexpected results in Guardium reports, configure your policy rules to handle depth by using tuples.

Cannot modify the receiver table for an Audit Process after it has been executed at least once

If you cannot modify the receiver table for an audit process, clone the audit process and replace the original.

Symptoms

After an audit process runs at least once, you can neither remove nor add a receiver. You can also not modify the following properties for a receiver.

- Action Req.
- Cont.
- Appv. if Empty

Causes

After an Audit Process runs at least once, the receiver table is locked and you cannot modify most of the properties.

Environment

All Guardium configurations (collector, aggregator, central manager) are affected.

Resolving the problem

The following steps enable you to modify the receiver table.

1. Clone the audit process.
2. Make changes to the cloned audit process.
3. Delete the original audit process. However, if you do not want to lose the audit process history, you can rename the audit process.
4. Rename the cloned audit process to the name of the original one.

Cannot see multi-byte characters

If you export a Guardium report to PDF and the characters are not correct, switch the PDF font configuration.

Symptoms

You can view reports in the GUI. However, when you export the report to PDF, the characters are not correct or missing. The characters appear as question marks or other symbols in the PDF report.

Causes

The default font in Guardium PDF exports does not show multi-byte characters correctly. For example, Greek, Cyrillic, and Chinese characters do not display correctly.

Environment

The collector, aggregator, and central manager are affected.

Resolving the problem

In version 9 and later, switch the PDF font configuration to resolve the problem.

1. Log in as a user in the CLI.
2. Run the command **store pdf-config multilanguage_support**
3. Select **2 Multi-language**.

File system is almost full

If the Guardium file system is almost full, change the log rotation strategy.

Symptoms

The file system is filling up and approaching 100%.

Causes

Alerts and reports are sent to the syslog and can fill up the file system.

Environment

The collector or aggregator might be affected.

Resolving the problem

By default, the log files rotate weekly and keep five files. However, you can change the log rotation strategy for the log files. Use the following command to keep fewer messages in the system.

```
support logrotate [agg|message] [daily|weekly|monthly] [# of rotations]
```

Guardium audit reports viewed in Microsoft Excel have rows with unexpected characters

If you view an Audit report in .csv and see rows with unexpected characters, use another .csv viewer or view it as a .pdf file.

Symptoms

When you view an Audit report (in .csv format) in Microsoft Excel, you notice that certain rows are filled with unexpected characters. The characters might look similar to what you find in the full SQL column. The problem is not seen in .pdf reports or in GUI reports.

Causes

Microsoft Excel has a limit on what a cell can contain of 32,767 characters. If your captured SQL is longer than this limit, it will spill over onto the next row.

Environment

The Collector, Aggregator, and Central Manager are affected.

Resolving the problem

Use another .csv viewer that has a larger limit on characters per cell or view the audit report as a .pdf file instead.

Reports show IP address as 0.0.0.0

Symptoms

The IP address shows as 0.0.0.0 in Guardium.

Causes

While Guardium is decrypting the traffic, the IP address is initially recorded as 0.0.0.0 because the sniffer does not know what the actual IP address is. After the decryption is completed, a separate thread repopulates the session tables with the correct IP address.

Environment

Any database that encrypts the database traffic is affected.

Resolving the problem

Run the same report after a few minutes. To view the correct client IP for newer traffic, add the field Analyzed Client IP from the client/server domain to the report. It is possible that for some rows, the Analyzed Client IP is blank. If it is blank, the decryption for that piece of traffic is not completed.

Request was interrupted or quota exceeded error message

If you receive an error message that states the request was interrupted or the quota was exceeded when you run a report, divide the report into pieces of shorter reporting interval.

Symptoms

When you run a report in Guardium, you receive the following error message.**Request was interrupted or quota exceeded**.

Causes

The error message **Request was interrupted or quota exceeded** appears when an interactive report does not complete within the 3-minute time limit. The underlying cause is generally the size of the report.

Environment

The collector and aggregator are affected.

Resolving the problem

When encountering this problem, it usually indicates that the report is too large to run in interactive mode. The best practice is to run large reports as an audit process instead. For more information, see [Building audit processes](#).

Scheduled Job Exceptions every 5 minutes

If you receive a Scheduled Job exception every 5 minutes, deactivate the alert from the Anomaly Detection page.

Symptoms

You receive the same message in the Scheduled Jobs Exceptions report at regular short intervals, typically every 5 minutes. This interval is the same as the polling interval that anomaly detection runs on.

An example of the Scheduled Jobs Exceptions report might look like the following.

Timestamp	Exception Description	Count of Exceptions
2013-12-05 15:51:22.0	java.lang.NumberFormatException: empty String	1

The same exception appears every 5 minutes.

Causes

One of the active alerts is causing the error.

Environment

Guardium collectors and the Aggregator are affected.

Diagnosing the problem

You can check the polling interval and active alerts in the Anomaly Detection page. Click Protect > Database Intrusion Detection > Anomaly Detection to open the Anomaly Detection page.

Resolving the problem

Identify the exact alert that is causing the problem and deactivate it.

1. Deactivate one alert from the Anomaly Detection page.
2. Wait for the length of the polling interval to elapse.
3. Check to see whether the errors stop with that alert deactivated.
4. If not, reactivate the alert and deactivate the next one.
5. Repeat steps 2-5 until you try all alerts.

If you find the alert that is causing the problem and need assistance to understand or stop the error, contact IBM Guardium Technical Support and provide the following items:

1. The exact error text and screen capture.
2. Output of the following CLI commands. If requested, specify the length of one polling interval.

```
support must_gather app_issues  
support must_gather alert_issues
```

Scheduled jobs exception: merge required, delay executing process

If you receive an error message that states merge required, delay executing process, reschedule the Audit process.

Symptoms

You receive the following message. **Merge required, delay executing Process**. You might receive several of these messages over a short period.

Causes

The audit process requires the merge process to finish before it can run.

Environment

The aggregator is affected.

Diagnosing the problem

Click Reports > Guardium Operational Reports > Aggregation/Archive Log to open the Aggregation/Archive Log. You can also diagnose the problem in agg_progress.log.

Resolving the problem

Reschedule the audit process to run at least 10 minutes after the merge process.

The database user is not shown correctly in Guardium reports when you monitor Teradata

If Guardium reports do not show the database user correctly when you monitor Teradata, configure the Teradata Database.

Symptoms

When you view records from the monitored Teradata Database in Guardium reports, the database user name field does not show up as expected. The user name is truncated or missing.

Causes

The Teradata Database is not enabled to return the full user name.

Environment

Any Guardium collector that captures data from the Teradata database is affected.

Resolving the problem

Use the following command to enable the Teradata Database to return the full user name, in the correct character set, to the monitoring application. Other applications are not affected.

gtwcontrol -u yes -d

The -d command displays the updated GDO settings.

Note: This setup returns the user name in unencrypted form. If encryption is enabled, the system returns an error message.

Unexpected results in Guardium reports with embedded commands

If you receive unexpected results in Guardium reports, configure your policy rules to handle depth by using tuples.

Symptoms

You see results in your reports that you do not expect or that you believe should be filtered out by the policy. Conversely, you do not capture statements that you expect to capture.

Causes

The SQL usually has several objects and commands that are embedded in the statement. The policy or report definition is not configured to deal with objects or commands at different depths.

Environment

Guardium collectors are affected.

Resolving the problem

Verify that your conditions match the correct object name. Use the correct main entity to show objects or SQL verbs at different depths. If you still see unexpected behavior, use the group builder to define a group of tuples to use in the policy. A tuple allows multiple attributes to be combined to form a single group member.

Note: Tuple supports the use of one slash and a wildcard character (%). It does not support the use of a double slash.

Troubleshooting Guardium® Data Protection issues with assessing and hardening an environment

These sections present troubleshooting and solutions for common problems with assessing and hardening.

- [CAS is not working with Java 1.7 on Windows](#)

If Guardium change audit system is not working with Java version 1.7 on Windows, copy msver100.dll to your CAS bin folder.

- [Vulnerability Assessment exception group members appear in failed test](#)

If members of a test exception group appear in a failed vulnerability assessment test, use an escape sequence for the backslash character.

CAS is not working with Java 1.7 on Windows

If Guardium change audit system is not working with Java version 1.7 on Windows, copy msver100.dll to your CAS bin folder.

Symptoms

Guardium CAS works with older Java versions but not with Java 1.7.

Causes

msver100.dll is missing from <GUARDIUM STAP directory>\cas\bin\

Environment

Guardium CAS on Windows is affected.

Resolving the problem

To resolve the problem, complete the following steps.

1. Find the path where Java 1.7 is installed on your system such as C:\Program Files (x86)\Java\jre7\bin
2. Find the location of the library jvm.dll within the Java path found in the previous step.
3. Edit the cas.cfg file in the <CAS directory>\conf directory. For example, C:\Program Files (x86)\GUARDIUM_STAP\cas\conf\cas.cfg is a typical file path.
4. Find the line corresponding to the JVM such as ;JVM=c:\program files\java\jre1_2_3\bin\client\jvm.dll.
5. Remove the semicolon from the beginning of the line. Then, set the JVM to the path of the library jvm.dll in step 2. **JVM=C:\Program Files (x86)\Java\jre7\bin\server\jvm.dll**.
6. Copy msver100.dll from the bin folder in your Java 7 installation directory to your <CAS directory>\bin folder. For example, copy C:\Program Files (x86)\Java\jre7\bin\msver100.dll to C:\Program Files (x86)\Guardium\GUARDIUM_STAP\cas\bin\msver100.dll.
7. Restart the change audit system.

Note: This is only needed for Java version 1.7. For older versions of Java, this step is not needed.

Vulnerability Assessment exception group members appear in failed test

If members of a test exception group appear in a failed vulnerability assessment test, use an escape sequence for the backslash character.

Symptoms

Some members of a test exception group appear in the details field when you run a vulnerability assessment. The group contains members with a backslash character and a REGEX tag such as **(R) US\John Doe.**

Causes

Special characters can trigger errors when Guardium parses the exception group.

Environment

Guardium collectors are affected.

Resolving the problem

Use an escape sequence for the backslash character or do not use the REGEX tag (use an exact match). Either of these examples work.

`US\John Doe`

`(R) US\\John Doe`

The REGEX tag (R) is used to trigger a regular expression search of the details field to remove any string that matches the regular expression. A backslash or any other character that has a meaning in a regular expression needs a backslash escape sequence to avoid parsing errors. If you do not use the (R) tag, the group member must exactly match the entire line in the details field for Guardium to make a match. To pass the vulnerability test, the details field of the test must be empty.

Troubleshooting Guardium Data Protection configuration

These sections present troubleshooting and solutions for common problems with configuring your Guardium® system.

- [Cannot configure STAP after upgrade](#)
Configure S-TAP in Guardium after you upgrade S-TAP.
- [Guardium fails to recognize the network device VMXNET x](#)
If Guardium fails to recognize the network device VMXNET x, install Guardium on a virtual machine and add the network adapter.
- [Guardium network interface error after system board replacement](#)
If you receive an error message after a hardware repair, reset the network parameters.
- [SSLv3 is enabled](#)
If you receive a warning that `SSLv3 is enabled`, disable SSLv3 to prevent the POODLE exploit.

Cannot configure STAP after upgrade

Configure S-TAP in Guardium after you upgrade S-TAP.

Symptoms

After you upgrade S-TAP using the Guardium Installation Manager (GIM), you cannot configure the database path parameters in the Inspection Engine in Guardium even though the installation results for the module show as successful.

Causes

K-TAP is not properly upgraded if the new S-TAP is installed as a fresh module. Because the old K-TAP module is not removed, there is a protocol mismatch between the old K-TAP module and the new S-TAP.

Environment

S-TAP installed in UNIX and Linux such as AIX, HP-UX, Linux, and Solaris.

Diagnosing the problem

To diagnose the problem, run the `guard_diag` utility to collect must gathering data for Guardium S-TAP.

The following lines are seen in the syslog file.

```
STAP and KTAP Protocol Version Mismatch,  
Exit!!!!: No such file or directory  
Tap_controller::init failed  
GUARD-01: Error Initializing STap
```

The modules log file lists the old K-TAP. For example: `ktap_24276
338760 0`

Resolving the problem

To resolve the problem, follow these steps in the GIM modules installation pane.

1. Set K-TAP Live Update to Y.
2. Set K-TAP_ENABLED to Y and reinstall the new S-TAP.

Guardium fails to recognize the network device VMXNET x

If Guardium fails to recognize the network device VMXNET x, install Guardium on a virtual machine and add the network adapter.

Symptoms

Guardium fails to recognize the network device VMXNET x during the installation on VMware. You receive the error `eth0: unknown interface: No such device` when you install Guardium on VMware as a guest. The error message appears after you restart the system.

Causes

VMXNET x virtual network adapter requires a specific driver that is only contained in VMware tools and no operating system has the driver. Guardium is running on Linux and the installer does not have a driver for VMXNET x.

Environment

The Guardium system is affected.

Resolving the problem

Resolve the problem by completing the following steps.

1. Create a virtual machine on VMware by using a default network adapter such as E1000 or Flexible.
2. Install Guardium on the virtual machine.
3. Install the current GPU cumulative patch for Guardium.
4. After the installation, log on to the CLI console and run the command `setup vmware_tools install` to install VMware tools.
5. Shut down the Guardium system from the CLI console with the command `stop system`.
6. Edit the virtual machine settings with a VMware client tool such as VMware Infrastructure Client. Select the current network adapter and remove it.
7. Add the network adapter called VMXNET.
8. Restart the Guardium system.

Guardium network interface error after system board replacement

If you receive an error message after a hardware repair, reset the network parameters.

Symptoms

After a hardware repair such as replacing the system board on the Guardium appliance, the network connectivity is lost. The following error message occurs for each network interface when the appliance is rebooted.

`rtnetlink answers: no such device`

Causes

After you replace the system board, the MAC address will change. This change causes a disparity between the actual MAC address and what is stored in the interface configuration files.

Environment

Any Guardium appliance (collector, aggregator, or central manager) on which the system board has been replaced and all Guardium versions are impacted.

Resolving the problem

Log in to the appliance from the console as user CLI and reset the network parameters by running the following commands.

```
store network interface reset
store network interface ip <IPv4 or IPv6 address>/prefix
store network routes defaultroute <IPv4 or IPv6 gateway address>
store network resolvers <IPv4 or IPv6 address> [IPv4 or IPv6 address] [IPv4 or IPv6 address]
restart network
```

If the problem is still not resolved, contact Guardium Support for manual intervention.

SSLv3 is enabled

If you receive a warning that `SSLv3 is enabled`, disable SSLv3 to prevent the POODLE exploit.

Symptoms

You receive the following warning: **SSLv3 is enabled.**

Causes

SSLv3 contains a protocol vulnerability known as Padding Guardium® On Downgraded Legacy Encryption (POODLE). If SSLv3 is enabled on your system, this vulnerability allows attackers to force an SSL/TLS fallback to SSLv3, break the encryption, and intercept network traffic in plaintext. The vulnerability is detailed in the National Vulnerability Database as CVE-2014-3566.

Guardium recommends disabling SSLv3 on all systems to prevent the POODLE exploit, and SSLv3 is disabled by default on new Guardium systems. However, older systems and some upgrade scenarios may leave SSLv3 enabled.

This topic describes how to check the status of SSLv3 and disable it if necessary.

Attention: Disabling SSLv3 can disrupt connectivity between a Guardium v10 Central Manager and some managed units running Guardium v9 before GPU 500. If you have a mixed environment with managed units running Guardium v9 before GPU 500, either upgrade the managed units to GPU 500 or apply patch 9501 before disabling SSLv3.

Resolving the problem

1. Verify the status of SSLv3 using the following CLI command: **show sslv3**.
 - If the output indicates **SSL setting is disabled**, SSLv3 is disabled. No additional steps are required to disable SSLv3.
 - If the output indicates **SSL setting is enabled**, SSLv3 is enabled. Continue with this procedure to disable SSLv3.
2. Disable SSLv3 using the following CLI command: **store sslv3 off**. The command output should be similar to the following:

```
Current SSL setting is enabled. Will change to disabled.  
Restarting gui  
Changing to port 8443  
From port 8443  
Stopping.....  
ok
```

3. Verify that SSLv3 is now disabled: **show sslv3**. The output should now indicate **ssl setting is disabled**.

Access management

These sections present troubleshooting and solutions for common problems with access management.

- [Cannot log in to Guardium except as admin or accessmgr](#)
If you cannot log in to the Guardium GUI except admin or accessmgr, check the authentication configuration settings.
- [Guardium accessmgr password reset](#)
If you lose the accessmgr password and cannot log in, contact Guardium support.
- [Guardium CLI password reset](#)
If you lose the cli or guardcli1 - guardcli9 passwords and cannot log in, follow this procedure to reset the passwords.

Cannot log in to Guardium except as admin or accessmgr

If you cannot log in to the Guardium GUI except admin or accessmgr, check the authentication configuration settings.

Symptoms

You are unable to log in to Guardium with any user except admin or accessmgr. You see an invalid user name or password error despite using the correct user and password as defined by accessmgr. You receive the following error message. **Invalid user name and/or password. Please reenter your credentials..**

Causes

The authentication setting is not configured as local.

Environment

The collector, aggregator, and central manager are affected.

Resolving the problem

To solve the problem, change the authentication setting to local. This action enables you to log in as any user defined in the accessmgr.

Guardium accessmgr password reset

If you lose the accessmgr password and cannot log in, contact Guardium support.

Symptoms

You lost the Guardium accessmgr password and cannot log in to the GUI. The account is also locked after successive failed attempts.

Causes

Guardium prohibits multiple failed login attempts.

Environment

The collector, aggregator, and central manager are affected.

Resolving the problem

Log in to the CLI and run the following command: **support reset-password accessmgr**.

```
G10.ibm.com> support reset-password accessmgr
Password for accessmgr account have been successfully reset using keyword:<passkey>
Please provide these number to Guardium Customer Service to receive actual account password.
ok
```

After you receive the new password, unlock the account.

1. Use the following command to unlock the account. **unlock accessmgr**.
2. Log in as accessmgr and edit the accessmgr details to enter a temporary password.
3. Log in again with the temporary password.
4. When you are prompted, enter a new password.

Guardium CLI password reset

If you lose the *cli* or *guardcli1 - guardcli9* passwords and cannot log in, follow this procedure to reset the passwords.

Symptoms

You lost the Guardium the *cli* or *guardcli1 - guardcli9* passwords or otherwise cannot log in to the command line interface and need to reset the passwords.

Environment

This condition and its resolution apply to Guardium collectors, aggregators, and central managers as well as to standalone systems.

Resolving the problem

Use the following procedure to reset CLI account passwords:

1. Open a Guardium VM console and log in as the *rescue* user. You must use the Guardium console: remote SSH access is not allowed for the *rescue* account.
2. Upon logging in, the console displays a single-use passkey. Record this passkey.
3. Contact IBM support and provide the *rescue* user passkey. IBM will decode the passkey and return a single-use password for the *rescue* user.
4. Log in as the *rescue* user using the decoded password provided by IBM.
5. Reset CLI account passwords using the following command (where <username> is *cli* or *guardcli1 - guardcli9*):

```
reset password cli_user <username>
```

Note:

- The *rescue* user passkey is immediately reset after a successful log in. However, if the console times out before the rescue passkey is decoded and used, simply log in again as the *rescue* user and the same passkey is displayed.
- The *rescue* user can also retrieve passkeys or reset passwords for the *root* and *cloudsupport* users using commands equivalent to a standard CLI account:

Rescue command	CLI command
show passkey root	support show passkey root
show passkey cloudsupport	support show passkey cloudsupport
reset password root	support reset-password root
reset password cloudsupport	support reset-password cloudsupport
reset password cli_user	n/a

Aggregation

These sections present troubleshooting and solutions for common problems with aggregation.

- [Cannot convert Guardium collector to aggregator](#)

If you cannot convert a Guardium collector to a Central Manager aggregator, reinstall Guardium and select aggregator during installation.

- [Data Export configuration change from a Guardium managed system's GUI fails with error](#)
If a Data Export configuration change fails, make sure that the shared secret key is the same on the collector and aggregator.
- [Difference between audit process results and report](#)
If there is a difference between your audit process results and the report, check that all appliances are set to the same timezone.
- [HY000 errors after restoring the configuration in an aggregator](#)
If you receive HY000 errors after you restore the configuration in an aggregator, run a dummy import.
- [UI banner warning: Data not exported or archived](#)
- [Health alerts and UI banner warning: Old partitions found](#)

Cannot convert Guardium collector to aggregator

If you cannot convert a Guardium collector to a Central Manager aggregator, reinstall Guardium and select aggregator during installation.

Symptoms

You try to convert a Guardium collector to an aggregator with the command **store unit type manager aggregator**.

However, the following command shows that the unit type is still listed as manager.

```
> show unit type  
Manager
```

Causes

A collector cannot be converted to an aggregator with a CLI command.

Environment

Guardium collectors are affected.

Resolving the problem

To convert a collector to an aggregator, reinstall the Guardium product and select aggregator as the unit type during installation. After you install the aggregator, you can convert it to a central manager aggregator with the command **store unit type manager**.

Data Export configuration change from a Guardium managed system's GUI fails with error

If a Data Export configuration change fails, make sure that the shared secret key is the same on the collector and aggregator.

Symptoms

You attempt to save new settings for the data export and get the error when you click Apply to save the configuration:

Please correct the following errors and try again:
A test data file could not be sent to this host with the parameters given. Please confirm the hostname or IP address is entered correctly, the host is online, the target directory exists and can be written to by the user given, and the password given is correct for that user.

Causes

Guardium attempts to log in with scp to the target host with the user and password that are specified in the Data Export configuration. Then, Guardium attempts to copy a test file to the target directory. The shared secret on this system does not match the Shared Secret on the aggregator you are trying to set this system to export to.

Environment

The Guardium configurations: collector and aggregator are affected.

Resolving the problem

Make sure that the shared secret key is the same on the collector and aggregator. You can use one of the following methods:

1. If you know the shared secret on the aggregator, set the shared secret on the collector to the same value. You can use one of these methods:
 - From CLI: use command **store system shared secret** to set the Shared secret key
 - From GUI, set the shared secret key under Setup->System->System Configuration.
2. Back up the current shared secret on the aggregator and restore it to the collector.
 - On the aggregator, run the CLI command.

```
aggregator backup keys file <user@host:/path/filename>  
Parameters  
user@host: /path/filename
```

For the file transfer operation, specify a user, host, and full path name for the backup keys file. The user that you specify must have the authority to write to the specified directory.

- On the collector, run this command to restore the shared secret key:

```
aggregator restore keys file<user@host:/path/filename>
```

3. Reset the shared secret for both appliances to be the same.

Note: If you change the shared secret for the aggregator, you need to reset the shared secret for all other Guardium systems that export to it.

Difference between audit process results and report

If there is a difference between your audit process results and the report, check that all appliances are set to the same timezone.

Symptoms

You set a report to run on the aggregator as part of an audit process with time parameters, for example, Start of Last Day and End of Last Day. When you look at the results of that report, the first time stamps are always at a set time after 00.00 for example, 02.00. Additionally the last time stamps are always at a set time before 23.59 for example, 21.59. However, when you run the report interactively, the time stamps are shown as expected.

Causes

The collector and aggregator time zones might not be set the same.

Environment

The aggregator is affected.

Diagnosing the problem

Check that all appliances are set to the same timezone. Use the following command. `show system clock timezone`.

Resolving the problem

If the collector and aggregator are not set in the same timezone, configure the timezone of the appliances with the CLI.

```
store system clock timezone list  
store system clock timezone <timezone>
```

Verify that the time is correct on the appliance with the following commands.

```
show system clock datetime  
store system clock datetime
```

You can also synchronize the datetime by using the following commands to manage the time server.

```
show system time_server all  
store system time_server state  
store system time_server hostnames
```

HY000 errors after restoring the configuration in an aggregator

If you receive HY000 errors after you restore the configuration in an aggregator, run a dummy import.

Symptoms

When you restore the configuration of an aggregator or the Central Manager, you receive one or both of these messages.

```
ERROR 1031 (HY000) at line 1: Table storage engine for 'GUARD_USER_ACTIVITY_AUDIT' doesn't have this option  
ERROR 1031 (HY000) at line 1: Table storage engine for 'AGGREGATOR_ACTIVITY_LOG' doesn't have this option
```

Causes

This error condition can occur if there is a temporary mismatch in the internal databases.

Environment

The collector and aggregator are affected.

Resolving the problem

To resolve the problem, run a dummy import.

UI banner warning: Data not exported or archived

Symptoms

After logging into Guardium UI, a banner warning shows Data not exported or archived: [n] days have not been exported or archived and do not meet the purge criteria. Export or archive process failures may be seen in the UI Aggregation/Archive log, and the Days not exported or archived report may indicate missed days.

Causes

Days older than the purge period plus 30 days exists on the system and has not been exported or archived. Allow purge without exporting or archiving is not selected.

Environment

The condition may apply to Guardium collectors and aggregators.

Resolving the problem

1. Check the Days not exported or archived report. For more information, see [Viewing days whose data was not archived or exported](#).
Note: Note this report shows all days that have not been exported or archived. It is not limited to days older than purge age plus 30 days.
2. Decide whether you need to export or archive any of the days indicated in the report, considering the days age and contents.
3. Using the Archive data older than and Ignore data older than values from the report, export or archive the appropriate days. Or, if the days indicated in the report are not needed, select Allow purge without exporting or archiving and run the purge.

Health alerts and UI banner warning: Old partitions found

Symptoms

The condition is marked by the following symptoms:

- The Deployment Health Dashboard on a central manager shows events with the name Old Partitions Found. The events may come from one or many managed units or from the central manager itself.
- After logging into the Guardium UI, a UI banner warning shows Old partitions found: Oldest partition found: p[date].

Causes

The symptoms appear when old partitions exist on the internal system database. The severity of the alert corresponds to the age of the partitions, and the default values are as follows:

- Medium severity: partitions older than the purge age plus 62 days
 - A UI banner warning shows on all systems with a medium severity alert
- High severity: partitions older than the purge age plus 120 days
- Critical severity: partitions older than the purge age plus 240 days

The purge period of the system is shown on the Data Archive page of the Guardium UI, and the date of the oldest partition is shown in the details section in the format YYYYMMDD.

Note: The purge period is based on the ADDITIONAL_PURGE_AGE parameter. The default value is 60 days. Do not change this value without consulting Guardium support. There are several possible root causes for having old partitions on the system, for example:

- Days have not been archived or exported and therefore have not been purged
- Invalid timestamps are causing data to not be purged
- There are corrupted partitions that cannot be dropped by the purge process

Environment

The condition may apply to Guardium collectors, aggregators, and central managers.

Resolving the problem

Resolve the problem using the following guidance:

1. Resolve any existing Data not exported or archived: [n] days have not been exported or archived and do not meet the purge criteria UI banner warnings. These warnings will appear on units where days have not been exported or archived. For more information, see [UI banner warning: Data not exported or archived](#)
2. Upgrade to latest patch bundle. Known cases where purge could not clear partitions may be resolved in latest version.
3. If problem remains, resolution may depend on several factors:
 - How much data is on the Guardium system
 - How many old partitions exist
 - The root cause explaining the old partitions
 - Whether you have previously attempted to clean up the old partitions
 - How many Guardium systems are affected

Contact Guardium support to begin resolving this issue. Provide the following must gather information:

- support must_gather patch_install_issues

- support must_gather agg_issues
- support must_gather system_db_info

Note: The following document contains an internal section that Guardium support can consult to resolve the problem: [IBM Security Guardium v10.0p9998 health check errors - Data older than purge period or Old partitions found.](#)

Internal database

These sections present troubleshooting and solutions for common problems with the internal database.

- [Why is the Guardium internal database is filling up?](#)
If the Guardium internal database is filling up, you can purge the data manually or as part of the regular purge strategy.
- [Managed unit database is filling up](#)
Learn what you can do if your system database is filling up.
- [How to purge off some old audit results from the Guardium appliance](#)
The database is full. Old audit results need purging from the Guardium Appliance.
- [Resolving internal database full problems](#)
The Guardium internal database full percentage is not decreasing, even after a successful purge. Reclaim database space with **OPTIMIZE**.

Why is the Guardium internal database is filling up

If the Guardium internal database is filling up, you can purge the data manually or as part of the regular purge strategy.

Symptoms

- Cannot log in to GUI.
- tomcat error on GUI.
- Size of DB from System View approaching 100%.
- Receiving alerts that indicate the database size is getting larger.

Causes

The Guardium internal database can fill up for many reasons. For more information about a general approach to resolving the situation, see: [Managed unit database is filling up](#). Use the guidelines in [Resolving the problem](#) along with [Managed unit database is filling up](#) to help resolve the problem. If you are unable to take any of the actions, use the general steps in [Managed unit database is filling up](#) to lower the database size.

The reason that the internal database fills up can often be determined by analyzing the largest tables in the database. Each table has different processes that cause it to grow and different strategies for managing its size.

Resolving the problem

1. Check the largest tables in CLI. Enter: `support show db-top-tables all`
Example output:

Table	Size (M)	I/D %	Unused(M)	Est. Rows	Name
132526	17	22621	46144369	GDM_CONSTRUCT_TEXT	
20669	213	25	6738570	GDM_CONSTRUCT_INSTANCE	
19399	126	11	1051215	GDM_POLICY_VIOLATIONS_LOG	
1038	241	4	254991	REPORT_RESULT_DATA_ROW	
987	172	24	166504	GDM_SESSION	
860	29	0	516276	GDM_FIELD	
743	248	7	90036	GDM_OBJECT	

2. Start with your largest table. Use the actions to help reduce the size in the long term. The most common largest tables are listed here, with the causes for filling up, and the actions to stop the problem in the long term. The list is not exhaustive. Use this information along with an overall purging strategy.

GDM_CONSTRUCT_TEXT

Cause

- All data that is captured by a policy rule with Log full details action is written to this table.

Actions

- Use Log full details as little as possible in the policy. If this table is constantly filling up, review your reports and policy definition to ensure you are not capturing excess traffic with this action.

GDM_POLICY_VIOLATIONS_LOG

Cause

- All policy rules with alerting action, except Alert only write to this table, and they send alerts by the defined method (for example, Syslog). Correlation alerts log to this table if Log policy violation is selected in the definition.

Actions

- Review the alerting rules in your policy. Ensure that they are not alerting excessively, for example alert per match is not used simultaneously with alert once per session. If data needs to be forwarded to remote SIEM, but not seen in Guardium reports, use the action alert only.
- Check in the policy violations report Comply>Reports>Incident Management for the most common alerts. A recent change in the environment might cause a spike in alerts. For example, a new application might create thousands of failed login requests. Investigate the cause of the most common alerts and modify the policy if appropriate.

REPORT_RESULT_DATA_ROW

Cause

- The results of audit processes are stored in this table. They are only purged when:

- They are cleared from all receiver to-do lists.
- The conditions for removal in the definition are met. (By default the results of the last five runs are kept)

This table is not purged by a purge that is started in the GUI.

Action

- See [How to purge off some old audit results from the Guardium appliance](#).

One or more of GDM_CONSTRUCT, GDM_FIELD, GDM_OBJECT, GDM_SENTENCE

Cause

- The exception table can be filled with Guardium created exceptions (for example - parser errors) or exceptions from the monitored database (for example - SQL errors).

Actions

- Many types of exceptions are logged in this table. The first step is to identify which are the most common. You can use predefined reports in the Exceptions domain to find which exceptions are most common.
- The report Exceptions Type Distribution shows the number of each exception. Double-click the chart to drill down into further details, like a breakdown per server or client. You can also define your own query in the Exceptions Tracking domain. If the exceptions are coming from monitored traffic, consult with the service owner of that traffic in your organization. If not, you can contact Guardium support with details of your investigation.

Managed unit database is filling up

Learn what you can do if your system database is filling up.

Symptoms

- Cannot log in to GUI.
- tomcat error on GUI.
- The Used Disk: in the DB Utilization of the System Monitor page is approaching 100%.
- Receiving alerts that indicate the database size is getting larger.

Causes

Common causes are:

- Spikes in the captured data.
- A policy setting that allows logging of too much data in the internal database.
- Keeping too many days of data on the internal database.
- Collecting data from too many S-TAPs.

Resolving the problem

The quickest way to reduce the Used Disk: is to induce a purge of some older data now.

In this scenario Purge data older than 30 days is set, and you have all necessary backups and archives of your system. Now you want to purge off slightly more data.

1. Note the current Used Disk: in the DB Utilization of the System Monitor page.
2. Go to Manage > Data Management > Data Archive.
3. Set Purge Data Older than to 25 days.
4. Verify that the Purge checkbox is checked.
5. Verify that the Archive checkbox is cleared.
6. Verify that the Allow purge without exporting or archiving is checked.
7. Click Run Once now.
8. Check progress of the purge in Reports > Guardium Operational Reports >> Aggregation/Archive Log.
 - a. Right-click the Archive and select detail log.
 - b. Review the status of the purge process in the log.
9. When the purge is finished, note the current Used Disk: in the DB Utilization of the System Monitor page.

If the difference in the Used Disk: is in the right direction, then consider running the commands again for slightly fewer days. For example, purge older than 20 days.

- Remember to check the Archive checkbox when you complete these ad hoc purges.

Looking at the causes for this problem you might want to also consider:

- See the [Why is the Guardium internal database is filling up](#).
- Amend the policy to capture only the necessary data. For example, not all cases require capturing Full SQL.
- Switch one or more of the S-TAPs to another collector
- Amend the Archive and Purge settings to purge more data off each day.
- Ensure that the Schedule is set to run once per day.
- After you purge data, you might need to optimize the database. See [Resolving internal database full problems](#).
- If that does not help or you cannot access the GUI, contact Guardium Support.

How to purge off some old audit results from the Guardium appliance

The database is full. Old audit results need purging from the Guardium Appliance.

Symptoms

The database is full.

Causes

Normal purging of audit results is set in the audit process definition by the Keep for a minimum of x days or y runs option. Normal purging of audit results does not occur if the items in the Audit Process To-Do List were not handled or signed off. For example, if the To-Do List has items from 6 months ago, then no audit results since 6 months ago are purged.

Resolving the problem

Users must handle their To-Do Lists in a timely fashion, so the purging happens and the database does not fill up. Adding a Receiver is not mandatory when you create a new Audit Process. An Audit Process without a receiver can be used when results of the Audit Process are sent to the third-party application, and the Audit Process results do not need to be viewed or signed. If you still want to add a receiver but not require viewing or signing the Audit Process results, clear the To-Do List checkbox, but set the Email format field to Full Results (PDF or CSV). In this scenario, the status gets set to VIEWED and the receiver does not have to view the results to make them eligible for purge. If the To-Do List checkbox is cleared but the Email format field is set to None or Links only, the To-Do entry is created for the receiver because:

- These types of notifications do not set the status to VIEWED.
- The results cannot be purged.

The internal Guardium table **REPORT_RESULT_DATA_ROW** often gets large if the audit jobs or To-Do Lists are not handled or signed off.

Manual purge command

This command is a way to manually purge audit results. Use it only if the normal audit results purge is not working. It is recommended to contact Technical Support to understand why normal purge is not working. Use this command only when absolutely necessary to deal with audit tasks that produce a high number of records and take up too much disk space. Consult with Technical Support before you run this command. The response includes a warning message and a confirmation step.

- support clean DAM_data audit_results <start_date> <end_date>
- support clean DAM_data audit_results <end_date>

Resolving internal database full problems

The Guardium internal database full percentage is not decreasing, even after a successful purge. Reclaim database space with **OPTIMIZE**.

Symptoms

You can see whether the internal database is full in a number of ways:

- You recently purged data off the system but the data % did not decrease.
- The response to the CLI command **support show db-top-tables all** shows that the total size of the largest tables is much smaller than the total disk space available for the database.
- The syslog has messages that report a full database.
- Output of CLI command: **support show db-status used %**
- Mysql Disk Usage column in GUI>Guardium Monitor>Buffer Usage Monitor report.
- The output to the CLI command **support show db-top-tables all** shows a large amount of unused space (**Unused (M)**) in some tables.

Causes

The purge removed the data from the database, but did not necessarily reduce the size of the database files. Some database tables might need to be optimized to make the newly cleared space available.

Diagnosing the problem

Check the largest tables and database full percentage before and after you purge data by using CLI commands:

- support show db-status used %
- support show db-top-tables all

After the purge the largest tables sizes decreased significantly, but the database full % did not change. Also, the database might have a large amount of unused space. The numbers in this example are on a small test system. The columns, specifically the **Unused (M)**, shows how many Megabytes can be reclaimed. In this example, 7 MB of space can be reclaimed from **GDM_CONSTRUCT_TEXT**.

```
xxx.yyy.zzz.com> support show db-top-tables all
Table Size (M) | I/D % | Unused(M) | Est. Rows | Name
----- | ----- | ----- | ----- | -----
 1616 |    28 |      0 | 6038005 | REPORT_RESULT_DATA_ROW
   121 |    51 |      7 | 336557 | GDM_CONSTRUCT_TEXT
    13 |   223 |      4 | 21834 | GDM_CONSTRUCT_INSTANCE
     8 |    20 |      0 | 65149 | DB_ERROR_TEXT
```

Resolving the problem

Note: In live environments, it is only recommended to optimize when significant space (for example, 20 GB or more) can be reclaimed.

Optimize the internal TURBINE database tables as follows.

Note: The time to complete OPTIMIZE depends on the size of the underlying tables. And OPTIMIZE needs to stop the inspection-core. Run OPTIMIZE during a quiet time and let the command run to completion.

1. If the appliance is a collector, stop the inspection-core in the CLI.

```
stop inspection-core
```

2. Start the optimize process. The process might take up to several hours to complete depending on the size of the database tables. You can optimize the database in one of two ways.

- Optimize all tables, in the CLI, enter: diag, 4. Perform Maintenance Actions, 2. TURBINE Optimize.
- Optimize specific tables only. This might be appropriate if you know that a certain table has recently been heavily purged, and you can save time optimizing only one table. The CLI command is:

```
support optimize tables <database name> <table name>
```

For example:

```
support optimize tables TURBINE GDM_CONSTRUCT_TEXT
```

3. When the optimize is complete, enter:

```
start inspection-core
```

Example OPTIMIZE of one table that uses this method

You can see that 7 MB is reclaimed after the OPTIMIZE on that table is finished.

```
xxx.yyy.zzz.com> support show db-top-tables all
Table Size (M) | I/D % | Unused(M) | Est. Rows | Name
-----|-----|-----|-----|-----
 1616 |   28 |      0 | 6038005 | REPORT_RESULT_DATA_ROW
 121 |   51 |      7 | 336557 | GDM_CONSTRUCT_TEXT
 13 | 223 |      4 | 21834 | GDM_CONSTRUCT_INSTANCE
 8 |   20 |      0 | 65149 | DB_ERROR_TEXT
```

..etc...

```
No tables with more than 80% of free space used found.
ok
```

```
xxx.yyy.zzz.com> support optimize tables TURBINE GDM_CONSTRUCT_TEXT
This process can take some time, please wait...
Processing GDM_CONSTRUCT_TEXT...
TURBINE.GDM_CONSTRUCT_TEXT optimize note Table does not support optimize, doing recreate + analyze instead
TURBINE.GDM_CONSTRUCT_TEXT optimize status OK
ok
```

```
xxx.yyy.zzz.com> support show db-top-tables all
Table Size (M) | I/D % | Unused(M) | Est. Rows | Name
-----|-----|-----|-----|-----
 1616 |   28 |      0 | 6038005 | REPORT_RESULT_DATA_ROW
 122 |   51 |      0 | 350893 | GDM_CONSTRUCT_TEXT
 13 | 223 |      4 | 21834 | GDM_CONSTRUCT_INSTANCE
 8 |   20 |      0 | 65149 | DB_ERROR_TEXT
```

..etc..

```
No tables with more than 80% of free space used found.
ok
xxx.yyy.zzz.com>
```

Related concepts

- [diag CLI command](#)

Central management

These sections present troubleshooting and solutions for common problems with central management.

- [**A user is disabled in a Guardium managed unit, but shows as enabled on Central Manager**](#)

If a user is disabled in a Guardium managed unit but shows as enabled on Central Manager, run the Portal User Sync.

- [**Central Manager does not recognize the new version of upgraded units**](#)

If the Central Manager does not recognize the new version of upgraded units, select the upgraded units and refresh the page.

- [**Scheduled tasks do not fire at the scheduled time**](#)

If scheduled tasks do not fire at the scheduled time, schedule the import time to run after the portal user sync.

- [**Torque exception in Central Management view of GUI**](#)

If there is a torque exception in Central Management, delete the custom group and create a new group.

A user is disabled in a Guardium managed unit, but shows as enabled on Central Manager

If a user is disabled in a Guardium managed unit but shows as enabled on Central Manager, run the Portal User Sync.

Symptoms

A user is disabled in the managed unit. The user's account is re-enabled in the Central Manager but the user is still showing as disabled in the managed unit. The user's account shows as enabled in the Central Manager.

Causes

The user's account in the Central Manager is not synchronized with the managed unit.

Environment

A combination of the Central Manager, collector, or aggregator might be affected.

Resolving the problem

To synchronize the current user status between the Central Manager and the managed unit, run a Portal user sync.

1. Log in to the Central Manager as an admin user.
2. Click [Manage > Central Management > Portal User Sync](#) to open the Portal User Synchronization.
3. Click Run Once Now.

If the user's account between the managed unit and the Central Manager is still not synchronized, contact the IBM Guardium Technical Support for assistance.

Central Manager does not recognize the new version of upgraded units

If the Central Manager does not recognize the new version of upgraded units, select the upgraded units and refresh the page.

Symptoms

The Central Manager might not immediately recognize the new version of an upgraded aggregator or collector it manages. Pushing a patch from the Central Manager, which requires the new version, can result in an error that shows the unit is still at the previous version.

The managed unit's old version still displays in the Central Management view of the GUI. The unit ping times in that view, which implies good communication between the Central Manager and managed units.

Causes

The GUI needs to be refreshed to pull the new version information.

Environment

The Guardium Central Manager is affected.

Resolving the problem

In the Central Management view of the GUI, select the upgraded units and push Refresh. This action pulls the new version information from the units.

Scheduled tasks do not fire at the scheduled time

If scheduled tasks do not fire at the scheduled time, schedule the import time to run after the portal user sync.

Symptoms

Import fails and you receive the following message in agg_progress.log.

```
* 05/20 04:00:01 --- Import cannot start  
(guard_agg|turbine_backup.sh|restore_from_file.pl already running)  
* 05/20 20:00:46 --- Merge cannot start - aggregation still active
```

Causes

There is a conflict with the Central Manager portal user sync.

Environment

The aggregator is affected.

Diagnosing the problem

Find out which task is running in the background. Click [Reports > Guardium Operational Reports > Aggregation/Archive Log](#) to open the Aggregation/Archive Log.

Resolving the problem

To resolve the problem, schedule the import time to run after the portal user sync. Run the portal user sync every hour and the import time 30 minutes after that time.

Torque exception in Central Management view of GUI

If there is a torque exception in Central Management, delete the custom group and create a new group.

Symptoms

Selecting a certain custom group in the Central Management view of the Guardium GUI displays an error instead of the managed units in the group.

`org.apache.torque.TorqueException: Failed to select one and only one row.`

After the exception appears, it shows for any group or view under the Central Management tab. The exception even appears for groups that were previously working until you log out of the GUI and log back in.

Causes

This torque exception might occur if one of the managed units in the group was unregistered from the managed unit instead of the Central Manager.

Environment

Guardium Central Manager is affected.

Resolving the problem

Delete the custom group and create a new group that contains the same members.

S-TAPs and other agents

These sections present troubleshooting and solutions for common problems with S-TAPs and other agents.

- [Error opening shared memory area when you configure Guardium COMM_EXIT_LIST for DB2](#)
If you receive an error message when you configure Guardium COMM_EXIT_LIST, authorize the DB2 instance owner with the guardctl command.
- [Guardium fails to collect shared memory traffic from Informix](#)
If Guardium fails to collect shared memory traffic from Informix, check the inspection engine configuration.
- [High CPU and I/O Use in Guardium S-TAP host](#)
If you observe a high CPU or I/O usage, review the configuration for all of the inspection engines.
- [UNIX S-TAP cannot start: buffer size too large](#)
If a UNIX S-TAP cannot start, its buffer size might be too large.
- [S-TAP does not start automatically on Linux](#)
If the S-TAP agent for DB2 or Oracle does not start automatically on Linux, check for the /etc/event.d/ directory.
- [S-TAP returns not FIPS 140-2 compliant](#)
If you receive an error that about FIPS 140-2, change the configuration through the S-TAP Control page.
- [The K-TAP kernel module is still present after the uninstallation of S-TAP](#)
If the K-TAP kernel module is still present after the uninstallation of S-TAP, manually remove it.
- [Windows S-TAP service crashes on startup with error ID 1000](#)
If the S-TAP crashes with error ID 1000, check the SOFTWARE_TAP_IP parameter in the guard_tap_ini configuration file.
- [S-TAP is not capturing A-TAP traffic](#)
Use the A-TAP script to output detailed information on the A-TAP configuration.
- [Linux S-TAP is not capturing Db2 exit traffic](#)
Use the Db2 exit health check script to check and optionally fix the Db2 IE parameters.
- [Insufficient memory when installing UNIX S-TAP](#)
If you receive the following error: `modprobe: ERROR: could not insert 'ktap': Cannot allocate memory`, your system might not have enough memory.

Error opening shared memory area when you configure Guardium COMM_EXIT_LIST for DB2

If you receive an error message when you configure Guardium COMM_EXIT_LIST, authorize the DB2 instance owner with the guardctl command.

Symptoms

After you configure **DB2 COMM_EXIT_LIST** to use Guardium **libguard** and restart the DB2 server, you get the following error in the DB2 diag log.

```
2013-06-28-11.41.12.306169-300 E870950E486 LEVEL: Severe  
PID : 15764 TID : 139905833363200 PROC : db2sysc 0  
INSTANCE: db2001 NODE : 000
```

```
APPHDLL : 0-16
HOSTNAME: dbhost1
EDUID : 54 EDUNAME: db2agent () 0
FUNCTION: DB2 UDB, DRDA Communication Manager, sqljcCommexitLogMessage,
probe:234
DATA #1 : String with size, 91 bytes
WARNING: Shmem_access /.guard_writer0 failed Error opening shared memory area errno=2 err=8
```

Causes

The following message indicates that the Guardium library was unable to create the shared memory device that it requires.

```
Shmem_access /.guard_writer0 failed
Error opening shared memory area
errno=2
err=8
```

The DB2 instance owner must be added as an authorized user using the **guardctl** command.

Environment

Guardium collectors that use DB2 Exit (Version 10) Integration with S-TAP are affected.

Resolving the problem

The DB2 instance owner must be added as an authorized user by using the **guardctl** command.

1. Stop the DB2 instance.
2. Authorize the DB2 instance owner.
3. Start the DB2 instance.

If the Guardium Installation Manager (GIM) is not installed, authorize the DB2 instance owner with the following command.

```
<guardium_installdir>/bin/guardctl
authorize-user<db2 instance owner>
```

If the Guardium Installation Manager (GIM) is installed, authorize the DB2 instance owner with the following command.

```
<guardium_installdir>/modules/ATAP/current/files/bin/guardctl
authorize-user<db2 instance owner>
```

For example, if the DB2 instance owner is db2001 and GIM is installed in /usr/local/guardium, the command is
`/usr/local/gim/modules/ATAP/current/files/bin/guardctl`
`authorize-user db2001`.

Guardium fails to collect shared memory traffic from Informix

If Guardium fails to collect shared memory traffic from Informix, check the inspection engine configuration.

Symptoms

Guardium S-TAP does not collect shared memory traffic from Informix.

Causes

The inspection engine is not correctly configured.

Environment

Any S-TAP collection from any Informix system can be affected.

Resolving the problem

Check the inspection engine configuration under [Manage > Activity Monitoring > S-TAP Control](#). Ensure that the value in the Process Name field matches the result of the following command on the database server.

```
ls -lrt /INFORMIXTMP/.inf.*
```

Informix: /INFORMIXTMP/.inf.sqlexec Applies to all Informix platforms but Linux. For Informix with Linux, example: /home/informix11/bin/oninit

Informix must be running for this command to return a value.

For Linux servers using A-TAP, A-TAP must be configured to collect any shared memory traffic. Set the value to the same value as the --db-info parameter in the A-TAP configuration before you activate A-TAP.

High CPU and I/O Use in Guardium S-TAP host

If you observe a high CPU or I/O usage, review the configuration for all of the inspection engines.

Symptoms

You observe a high CPU or I/O usage by the Guardium S-TAP process.

Causes

The following items are common causes.

1. An error in the configuration of one of the inspection engines. If there are errors in an inspection engine, the S-TAP process restarts frequently or tries to reconnect to the inspection engine repeatedly.
2. The K-TAP portion of the S-TAP is sending connection information along with a confirmation request to the S-TAP. This step is causing delays.
3. ORACLE RAC is used, but the **unix_domain_socket_marker** parameter is not set in the S-TAP configuration file to avoid monitoring potentially large amounts of Oracle RAC traffic.
4. The User ID Chain (UID chain) feature is enabled, for example, **parameter hunter_trace=1** in the S-TAP configuration file. Hunter trace is used for UID chain and can be quite CPU intensive for S-TAP.
5. The firewall is enabled (**firewall_installed=1**). This firewall forces S-TAP to request verdicts for each new session that is observed which can hurt S-TAP performance.

Environment

All S-TAPs

Resolving the problem

Based on the cause, take the corresponding actions.

1. Review the configuration for all of the inspection engines and make sure that there are no errors in any of the parameters. For example, make sure the database installation directory, executable, ports, and any other parameters applicable to your inspection engine are correctly set with no misspellings or wrong values.
2. Set S-TAP configuration parameter **ktap_fast_tcp_verdict** to 1 (**ktap_fast_tcp_verdict = 1** in the **guard_tap.ini** configuration file) and restart the S-TAP. Here are the possible settings.
ktap_fast_tcp_verdict=0: KTAP confirms that the session is the database connection that the inspection engine configured by checking ports and Ips.
ktap_fast_tcp_verdict=1: KTAP does not send the request to S-TAP while the session's ports are in the range.
3. Disable the UID Chain feature if not needed by setting **hunter_trace=0** and restarting the S-TAP.
4. Set **firewall_installed=0** if SGATE is not needed and restart the S-TAP.

UNIX S-TAP cannot start: buffer size too large

If a UNIX S-TAP cannot start, its buffer size might be too large.

Symptoms

The S-TAP cannot start and issues the following messages:

```
mmap: Not enough space  
Can't initialize: Can't mmap buffer file /tmp/stabbuf/192.168.100.107.0.buf  
Error Initializing: Stab cannot initialize SQLGuard queue
```

Causes

The S-TAP is unable to allocate enough memory to match the buffer file.

Resolving the problem

Reduce the buffer file size for the S-TAP. The size is specified in the **buffer_file_size** parameter in the **guard_tap.ini** file.

You can also use the following formula to calculate the total memory that is used by the S-TAP buffers:

number of sqlguard main connections * buffer_file_size

For example, if you have 3 connections and **buffer_file_size** is set to 1 GB, then you need a total of 3 GB of memory for S-TAP buffers (3 *1GB = 3GB).

S-TAP does not start automatically on Linux

If the S-TAP agent for DB2 or Oracle does not start automatically on Linux, check for the **/etc/event.d/** directory.

Symptoms

The S-TAP process does not automatically start on Linux even though the **/etc/inittab** file shows a correct U-TAP entry.

Causes

Various Linux distributions such as RedHat 6 deprecated the use of the traditional init daemon that uses the etc/inittab file. They replaced it with an init process called upstart. Upstart uses the /etc/event.d and /etc/init directories for the automated start, stop, and respawn of processes such as U-TAP.

The S-TAP installer now checks for the existence of the /etc/event.d directory. If it exists, then entries in /etc/init are created for use by upstart. If it does not exist, then entries in /etc/inittab are created for use by the traditional init daemon.

If /etc/event.d is missing for any reason on a system with upstart, the inittab file is populated instead. The S-TAP process does not start or respawn when needed.

Environment

S-TAPs running on Linux are affected.

Resolving the problem

Check for the existence of the /etc/event.d/ directory.

If the /etc/event.d/ directory does not exist, complete the following steps to resolve the situation.

1. Uninstall the existing S-TAP installation.
2. Create the /etc/event.d dir as user root (mkdir /etc/event.d) .
3. Install the S-TAP.

S-TAP returns not FIPS 140-2 compliant

If you receive an error that about FIPS 140-2, change the configuration through the S-TAP Control page.

Symptoms

Supported: - Solaris X86 - Linux x86/64 - Linux x86/32 - Linux S390X - Linux IA64

Not Supported: - Solaris SPARC - AIX PowerPC - HPUX RISC - HPUX IA64 - Linux PowerPC

You see the following message in the S-TAP event log.

```
LOG_ERR: To enable FIPS  
140-2 mode set use_tls=1
```

Causes

FIPS 140-2 is a U.S. government security standard for cryptographic modules. If you see this message, it indicates that the S-TAP configuration does not meet government requirements.

Note: This message does not indicate that there is an error with the S-TAP.

Environment

Guardium S-TAP is affected.

Supported: Solaris X86; Linux x86/64; Linux x86/32; Linux S390X; Linux IA64

Not Supported: Solaris SPARC; AIX PowerPC; HPUX RISC; HPUX IA64; Linux PowerPC

Resolving the problem

To enable FIPS compliance, the guard_tap.ini file must have the following settings.

```
use_tls=1
```

You can change the configuration by using one of the following methods.

1. Click Manage > Activity Monitoring > S-TAP Control.
2. Modify the details section for the relevant S-TAP and use the TLS check boxes.
3. Restart the S-TAP.

You can also edit the guard_tap.ini file on the DB server directly and restart the S-TAP.

The K-TAP kernel module is still present after the uninstallation of S-TAP

If the K-TAP kernel module is still present after the uninstallation of S-TAP, manually remove it.

Symptoms

The K-TAP kernel module is still present after the uninstallation of S-TAP on a Solaris server.

Causes

The server did not restart properly to remove the K-TAP kernel module on Solaris servers.

Environment

Solaris

Diagnosing the problem

Check on the Solaris server by running both **modinfo | grep ktap** and **ls -al /dev/*tap***.

Resolving the problem

Manually remove the K-TAP kernel with the following steps.

1. Check that /etc/init.d/upguard is removed.
2. Remove /kernel/drv/sparcv9/ktap* and /kernel/drv/ktap*.
3. Run **modinfo | grep ktap** to get the name of the loaded driver.
4. Then, run **rem_drv<loaded driver>**. For example: **rem_drv ktap_36821**.
5. Remove /dev/ktap* and /dev/guard_ktap.
6. Restart the server.
7. Run **modinfo | grep ktap** to make sure that the driver is no longer loaded.
8. Remove GIM and gsvr entries from /etc/inittab (if you are using GIM only).
9. Manually clean up remaining files in /usr/local/guardium.

Windows S-TAP service crashes on startup with error ID 1000

If the S-TAP crashes with error ID 1000, check the SOFTWARE_TAP_IP parameter in the guard_tap_ini configuration file.

Symptoms

The S-TAP on a Windows server does not start. The Windows event log shows errors from Guardium S-TAP with event ID 1000.

```
Log Name: Application
Source: Application_Error
Event ID: 1000
Task Category: (100)
Level: Error
Keywords: Classic
Description:
Faulting application name: guardium_stapr.exe, version: 9.0.0.0
Exception code: 0x40000015
```

Causes

S-TAP cannot connect to the Windows system because the wrong SOFTWARE_TAP_IP is specified in the guard_tap.ini file.

Environment

Any Guardium S-TAP for Windows is affected.

Resolving the problem

Ensure the SOFTWARE_TAP_IP parameter in the guard_tap.ini configuration file matches the correct IP address of the Windows server. This parameter is passed on the installation CLI or in the IBM® Guardium® Installation Manager (GIM) parameters.

S-TAP is not capturing A-TAP traffic

Use the A-TAP script to output detailed information on the A-TAP configuration.

Symptoms

A-TAP traffic is not getting reported to Guardium.

Causes

Incorrectly configured IE parameters can prevent transmission of A-TAP traffic to the Guardium system.

Environment

Linux-type database server.

Resolving the problem

Use the A-TAP script to output details of the A-TAP configuration. The script is named **atap_must_gather.sh**. The script is located in the `guard_stap` bin directory. You can run it from anywhere with the full path.

The script runs a health check on each activated DB. The script output is written to a text file in the local `/tmp` directory, for example `/tmp/atap_must_gather.18-11-20_152824.txt`. Send this file to IBM Technical Support.

Linux S-TAP is not capturing Db2 exit traffic

Use the Db2 exit health check script to check and optionally fix the Db2 IE parameters.

Symptoms

Db2 Exit traffic is not getting reported to Guardium.

Causes

Incorrectly configured IE parameters can prevent Db2 Exit traffic from getting reported to the Guardium system.

Environment

Linux environment using Db2 Exit.

Resolving the problem

Use the Db2 exit script to check the Db2 IE configurations, and optionally to make any required fixes identified by the script. The script is located in the `guard_stap` bin directory. You can run it from anywhere with the full path. The script has two options: `./db2_exit_health_check.sh [check | fix]`

By default it performs the health check only. The fix option rectifies any IE parameters errors identified by the script. The script runs a health check on each DB section, performing the following:

1. Find exit ie in `guard_tap.ini` file
2. Validate `db_install_dir`
3. Find the db user and group
4. Check if the db user is authorized
5. Check if `db_install_dir` matches with `DB2_HOME` or `DB2 HOME`
6. Check if DB2 EXIT LIB is in place correctly
7. Check permission of DB2 EXIT LIB path and DB2 EXIT LIB
8. Check if DB2 EXIT LIB is updated with currently installed S-TAP
9. Check if DB2 EXIT LIB is loaded

The script output lists the problems found for each IE, and if you used the fix option, it presents the problem (`ERROR`), the corrective action taken (`ACTION`) and the results of the corrective action. The output for a properly configured DB2 IE is `DB2 Exit IE in <DB name> has a GOOD setup.`

User response: Optional. When you have particular actions that are performed by particular users, use one or more of the `ts*Response` elements.

Insufficient memory when installing UNIX S-TAP

If you receive the following error: `modprobe: ERROR: could not insert 'ktap': Cannot allocate memory`, your system might not have enough memory.

Symptoms

When trying to install S-TAP, K-TAP fails with the following error `modprobe: ERROR: could not insert 'ktap': Cannot allocate memory`.

Causes

The K-TAP installation can fail when the kernel has insufficient memory. This kind of error usually indicates that there is system resource issue on the server.

Environment

Any Guardium Linux-UNIX S-TAP.

Resolving the problem

Make sure that your system has sufficient kernel memory allocated.

Collectors

These sections present troubleshooting and solutions for common problems with collectors.

- [Nanny process is killing sniffer](#)
If the nanny process is killing the sniffer, you might have too much traffic coming in.
- [Sniffer cannot connect to UNIX S-TAP](#)

Nanny process is killing sniffer

If the nanny process is killing the sniffer, you might have too much traffic coming in.

Symptoms

A message similar to the following is reported one or more times in Guardium system log (messages) or Alerts:

Nanny process error condition. The nanny process killed the sniffer. VmData was *number* and was over the limit.

Causes

The sniffer memory usage reached over 90% of the available memory and the nanny process has restarted it, which is expected behavior of the product.

Environment

Guardium collector

Resolving the problem

If you are observing this message frequently, there is too much traffic coming to the Guardium system. Reduce traffic to this Guardium system to resolve this message. For example, you may move some STAPs to a collector with less load, ignore some traffic in your policy, or implement load balancing to spread the traffic among more than one collector.

If the message is observed on very few occasions, it is most likely a momentary spike in traffic. To resolve the message, identify the reason for the spike and avoid the trigger. For example, you can review which processes were running at that time, identify the ones generating more traffic. If this message always coincides with a particular process or processes running, reduce the concurrent traffic at that time. For example, you can move heaviest process to run at a different time, or ignore some of this traffic through a policy.

Sniffer cannot connect to UNIX S-TAP

Symptoms

When you specify a different number of threads, such as 20, by using the command `snif -t 20`, the sniffer cannot connect to the UNIX S-TAP. In the GUI console, the status of the S-TAP is inactive.

Causes

The sniffer starts with six threads by default. When the number of threads exceeds the limitation, the sniffer cannot connect to the UNIX S-TAP because of undefined behavior.

Environment

UNIX S-TAP is affected.

Resolving the problem

Reduce the number of threads to make sure that the connection can be established successfully.

Troubleshooting Guardium Installation Manager (GIM)

These sections present troubleshooting and solutions for common problems with GIM.

- [Error installing the Guardium Installation Manager \(GIM\)](#)
If GIM does not install properly, create the directory manually.
- [Guardium Installation Manager \(GIM\) service does not start in Windows](#)
If the Guardium Installation Manager (GIM) service does not start in Windows, reinstall GIM in a folder that is reserved for 32-bit applications.

Error installing the Guardium Installation Manager (GIM)

If GIM does not install properly, create the directory manually.

Symptoms

When you attempt to install the Guardium Installation Manager (GIM) on RHEL6, you see the following error message.

```
cp:  
cannot stat '/usr/local/GIM/modules/central_logger.log': No such file  
or directory Installation failed
```

Causes

Various Linux distributions such as RedHat 6 deprecated the use of the traditional init daemon that uses the etc/inittab file. They replaced it with an init process called Upstart. Upstart uses the /etc/event.d and /etc/init directories for the automated start, stop, and respawn of processes.

Environment

The Guardium Installation Manager (GIM) is affected.

Resolving the problem

To fix the issue, complete the following steps.

- Remove the partial GIM installation.
- Create the /etc/event.d directory manually with the command **mkdir /etc/event.d**
- Run the GIM installer.

Guardium Installation Manager (GIM) service does not start in Windows

If the Guardium Installation Manager (GIM) service does not start in Windows, reinstall GIM in a folder that is reserved for 32-bit applications.

Symptoms

After you successfully installed the Guardium Installation Manager (GIM) on Windows, you notice that the service is not running.

Causes

GIM is a 32-bit application. If you are using a Windows 64 bit, GIM might be installed in Program Files instead of Program Files(x86).

Environment

GIM is affected.

Resolving the problem

Install GIM in Program Files(x86) because it is a Windows folder that is reserved for 32-bit applications.

File activity

These sections present troubleshooting and solutions for common problems with file activity and classification.

- [File activity is not logged in investigation dashboard or reports](#)
- [File activity from removable disk is not logged in investigation dashboard](#)
- [File activity appears in reports but not the investigation dashboard](#)
- [Some files missing from classification results](#)
- [Partial file discovery \(entitlement\) results in reports and investigation dashboard](#)
Reports and investigation dashboard are not showing complete discovery (entitlement) results.
- [File classification results are missing from reports and investigation dashboard](#)
- [File activity logs](#)
Learn where the File activity monitoring (FAM) log files are located.
- [FAM bundle fails to install](#)
After installing the GIM client, the FAM bundle installation fails.

File activity is not logged in investigation dashboard or reports

Symptoms

There is no file activity logged in the investigation dashboard or predefined reports, such as: File Activities, File Entitlement, Files Count of Activity Per Client, Files Count of Activity Per Server, Files Count of Activity Per User, Files Privileges

Resolving the problem

Check the following:

- Verify the FAM license is installed and on UNIX servers the S-TAP is active.
- Make sure you are not logged in as root in your file server for activities. Activities from root, (UID0) are not logged by default.
- On Linux/AIX, check the file path specified in your policy rule. For example, /testdir/ monitors a file called testdir and not the files in a directory called testdir. Specify /testdir/* to monitor files in the testdir directory.
- On Windows, if you use domains and your policy rule specifies a user, make sure the domain is specified. For example, svldev\Maryjane instead of just Maryjane.

File activity from removable disk is not logged in investigation dashboard

Symptoms

File activity from removable disk is not logged in investigation dashboard

Environment

FAM_SCAN_EXCLUDE_REMOTE_DIRECTORIES is set to true

Resolving the problem

Install the file activity monitoring policy *before* mounting the removable disk.

File activity appears in reports but not the investigation dashboard

Symptoms

You see file activity in the predefined reports, but not in the investigation dashboard.

Resolving the problem

Verify the configuration using the guard API:

- To send crawled data to quick search: `grdapi enable_fam_crawler activity_schedule_interval=2 activity_schedule_units=MINUTE entitlement_schedule_interval=10 entitlement_schedule_units=MINUTE`
- To enable quick search (with option to also include violations): `grdapi enable_quick_search includeViolations=true schedule_interval=2 schedule_units=MINUTE`

Some files missing from classification results

Symptoms

Some files are missing in the classification results.

Causes

The following are file types are *not* supported for classification: DAT, JPG, JPEG, GIF, TIF, TIFF, BMP, WAV, MOV, MP3, MP4, AVI, MPG, WMA, WMV, P7S, XFDL, XFD, FRM, JAR

Partial file discovery (entitlement) results in reports and investigation dashboard

Reports and investigation dashboard are not showing complete discovery (entitlement) results.

Symptoms

The discovery (entitlement) results that appear in reports and investigation dashboard is incomplete. Results for some files do not appear.

Resolving the problem

Verify that the document types and locations are included in your GIM configurations for discovery. Check the following GIM configuration parameters:

- FAM_SCAN_EXCLUDE_FILES
- FAM_SCAN_EXCLUDE_DIRECTORIES
- FAM_SCAN_EXCLUDE_EXTENSIONS
- FAM_SCAN_EXCLUDE_FILES
- FAM_SCAN_MAX_DEPTH

File classification results are missing from reports and investigation dashboard

Symptoms

File classification results are missing from reports and investigation dashboard.

Causes

Classification is an additional process that goes beyond metadata discovery.

Resolving the problem

Assuming your software requirements are met for the IBM Content Classification engine (<http://www-01.ibm.com/support/docview.wss?uid=swg27020838>) that is used for classification, verify the following GIM configurations:

- Ensure that the GIM parameter FAM_IS_DEEP_ANALYSIS= TRUE
- Verify that Decision Plan names are correct in FAM_ICM_CLASS_DECISION_PLANS setting and that the list of Decision Plans is delimited with a semicolon
- Verify that all listed Decision Plans (.dpn) files exist in the following location on the file server: %FAM_HOME%\conf\ContentClassification

User response: Optional. When you have particular actions that are performed by particular users, use one or more of the ts*Response elements.

File activity logs

Learn where the File activity monitoring (FAM) log files are located.

Symptoms

Cannot find FAM logs, or change debug level

Resolving the problem

FAM logs are located in:

- Windows: The FAM agent log file is called StapAT.ctl and resides in C:\Program Files\IBM\Windows S-TAP\Logs. The FAM installer log is C:\IBM Windows S-TAP.ctl drive. The Services logs are named FAMsvc.ctl and FsMonitor.ct, and are located in the log folder under the install path.
- Linux: FAM errors and debug logs are named guard_stap.fam.txt. The default location in UNIX is /tmp, and is configured by tap_log_dir. The debug level is configured by tap_debug_output_level.

FAM bundle fails to install

After installing the GIM client, the FAM bundle installation fails.

Symptoms

When attempting to install the FAM bundle, the system responds with a message similar to:

```
-1,GIM - Failure point : dependencyViolation (Dependency violation (FAM) : Missing mandatory dependency - STAP at GIM.pm line 3176, <MYFILE> line 20.)
```

Causes

The S-TAP bundle must be installed before installing the FAM bundle.

Environment

Relevant only in Linux / UNIX environments.

Resolving the problem

Verify the S-TAP for FAM is installed, then install the FAM bundle. See [Installing and activating file activity monitoring components](#).

Investigation dashboard

These sections present troubleshooting and solutions for common problems with the investigation dashboard.

- [Troubleshooting the investigation dashboard and enterprise search](#)

Use the GuardAPI to diagnose investigation dashboard and enterprise search issues.

Troubleshooting the investigation dashboard and enterprise search

Use the GuardAPI to diagnose investigation dashboard and enterprise search issues.

Symptoms

Enterprise search is enabled but the investigation dashboard is not showing full data; or a datamart is not exporting data as expected.

Causes

Causes can be any of:

- Enterprise search is not enabled.
- Firewall issue prevents communication between the central manager and the managed units.
- SSL exception prevents communication between the central manager and the managed units.
- Hardware on central manager is not sufficient to run enterprise search.
- Datamart is not extracted due to either error or missing schedule.
- Internal Guardium® search engine is down.
- Internal Guardium search engine did not upgrade successfully.

Diagnosing the problem

The GuardAPI command **test_solr** runs diagnostics on your system. The output indicates if there are any problems, and gives detailed instructions on resolving them. Follow the instructions provided. Here are three example of output.

Figure 1. Output to solr_test, no details, no issues reported

```
clusterMachineState: "No issues found."
```

Figure 2. Output to solr_test, with details, no issues reported

```
il-vm17.guard.swg.usma.ibm.com:
  isQuickSearchEnabled: "success"
  HardwareRequirementTest: "success"
  isSolrAlive: "success"
  ClusterConnectivity: "success"
  extractionStatus: "success"
  isClusterStateUp: "success"
  isThereClientSessionWarningInLog: "success"
  isThereSSLEceptionInLog: "success"
  isThereExceptionInUpgradeLog: "success"
```

Figure 3. Output to solr_test, no details, issue reported

JSON Raw Data Headers

Save Copy Collapse All Expand All Filter JSON

```

ClusterMachineState:
  ▶ 0: {...}
  ▶ 1:
    ip: "9.70.165.45"
    ▼ issue:
      ▶ 0:
        host: "sys-vm53.guard.swg.usma.ibm.com"
        unitType: "MU"
        success: false
        description: "Solr is down."
        ▼ recommendation:
          "Test Hardware requirements by executing: grdapi test_solr_hardware_requirement. If hardware is ok, execute grdapi get_solr_cluster_info and search in output file for the machine that's down in live nodes tag. If you can not find the live node for the machine, try to restart solr with CLI command: grdapi restart_solr."
    ▶ 2: {...}
  
```

Related reference

- [test_solr](#)

Troubleshooting Guardium Data Protection installation

These sections present troubleshooting and solutions for common problems encountered when installing your Guardium system.

- [**Checksum error during S-TAP installation**](#)
Follow these steps to rectify the download and transfer of the S-TAP installer file.
- [**Guardium S-TAP returns an illegal cp: option - f error message**](#)
If the S-TAP installation fails with cp: illegal option - f, run the command which cp and change the file path.
- [**Installing a new Guardium patch does not complete**](#)
If you cannot complete the installation of a new Guardium patch, stop the interfering process and reinstall the patch.
- [**Missing file or directory after new Guardium S-TAP installation**](#)
- [**Partition error installing Guardium**](#)
If you receive a partition error, select Custom installation and specify the disk location and size explicitly.
- [**Patch installation fails: No such file or directory**](#)
If the patch installation fails, check that the file matches the MD5SUM of the downloaded patch.

Checksum error during S-TAP installation

Follow these steps to rectify the download and transfer of the S-TAP installer file.

Symptoms

You receive an error similar to the following when you run the S-TAP installer to install Guardium S-TAP, indicating that either the md5 checksum or sha1 checksum is incorrect.

```
./guard-stap-v81_r26808_1-aix-6.1-aix-powerpc.sh
Verifying archive integrity...Error in checksums: 2082112805 is
different from 3728267449
```

Causes

The installer file is corrupted. The file became corrupted when the file was transferred to the database server or when the product was downloaded.

Environment

S-TAP on any server.

Resolving the problem

- If you are using FTP make sure it is set to binary mode.
- Try to transfer to the database server again.
- If that does not succeed, download the product again.

Guardium S-TAP returns an illegal cp: option - f error message

If the S-TAP installation fails with cp: illegal option - f, run the command which cp and change the file path.

Symptoms

The S-TAP installation fails with the following error message.

```
A directory called 'guardium' containing Guardium software needs to be created under a path provided.  
Enter the path prefix [/usr/local]? /opt/guardium  
Directory /opt/guardium/guardium/guard_stap does not exist, would you like to create it [Y/n]? Y  
Run STAP as root, or as user 'guardium' [R/u]? R  
Please be patient... This might take more than a minute.  
Copying installation files...  
cp: illegal option -- f  
UX:vxf5 cp: INFO: V-3-21462: Usage: cp [-i] [-p] f1 f2  
cp [-i] [-p] f1 ... fn d1  
cp [-i] [-p] [-r|-R] [-e { force | ignore | warn}] d1 d2
```

Causes

The path to /usr/bin/cp is different from what the installer expects.

Environment

The UNIX/Linux database server is affected.

Resolving the problem

Run the command **which cp**

If **which cp** returns a value other than /usr/bin/cp, run the command **export PATH=/usr/sbin:/usr/bin:\$PATH**.

Rerun the command **which cp** to confirm that the path is /usr/bin/cp.

Installing a new Guardium patch does not complete

If you cannot complete the installation of a new Guardium patch, stop the interfering process and reinstall the patch.

Symptoms

When you install a new patch it does not complete. The status column in the CLI command **show system patch installed** shows one of the following messages.

```
STEP: Setting "java" off  
STEP: Setting "amei" off  
STEP: Setting "sqlw" off
```

Causes

Tomcat, the inspection core, or another process on the machine interfered with the patch installation.

Environment

The Collector, Aggregator, and Central Manager are affected.

Resolving the problem

To install the new Guardium patch, stop any processes from interfering with the installation.

1. Delete the patch that is stuck by using the command **delete scheduled-patch**.
2. Restart the system by using the command **restart system**.
3. After the system restarts, stop the GUI and inspection core by using the commands **stop gui** and **stop inspection-core**.
4. Reinstall the patch and restart the GUI and inspection core by using the commands **restart gui** and **start inspection-core**.

Missing file or directory after new Guardium S-TAP installation

Symptoms

When you attempt to install S-TAP, you receive the following error message.

```
Tap_controller::init failed Opening pseudo device /dev/guard_ktap No such file or directory
```

In addition, /dev/*ktap* does not exist.

Causes

There are many possible reasons why the K-TAP device creation can fail. The following are the most common causes.

- You did not use the module files, including the K-TAP module for the Linux kernel.
- You did not specify the Flex Loading option to load the K-TAP module from the module files.
- A previous K-TAP module from an old installation is still running or installed.

Environment

All Linux and UNIX operating systems in which the IBM® Guardium® S-TAP product can be installed are affected.

Resolving the problem

To resolve the problem, take the following steps.

1. Run these commands as root.

```
<STAP directory>/KTAP/guard_ktap_loader stop  
<STAP directory>/KTAP/guard_ktap_loader uninstall  
<STAP directory>/KTAP/guard_ktap_loader install  
<STAP directory>/KTAP/guard_ktap_loader start
```

2. Check whether the K-TAP device is now created with the command **ls /dev/*ktap***. If it was created, issue is resolved. If not, continue to next step.
3. Stop the S-TAP process **guard_stap** if it is running. You can check whether it is running with command **ps -ef | grep guard_stap**.
4. Verify that the S-TAP process is not running with the command **ps -ef | grep guard_stap**.
5. Uninstall the S-TAP.
6. Confirm that the S-TAP directory is gone.
7. Check whether a K-TAP module is still running from an old installation. Use the appropriate command for your operating system.

```
Linux      : lsmod | grep ktap  
Solaris    : modinfo | grep tap  
HP-UX     : lsdev | grep tap  
AIX       : genkex | grep tap
```

If a device such as **ktap_<release>** is listed, then a K-TAP module is running.

8. If you find a K-TAP module is running in previous step, run the following steps to stop and uninstall the K-TAP module.

```
<STAP directory>/KTAP/guard_ktap_loader stop  
<STAP directory>/KTAP/guard_ktap_loader uninstall
```

Restart the server.

9. If you are using the Guardium Installation Manager (GIM), go to **Manage > Module Installation > Set up by Client**, select the client and click **Reset connection**. Wait for the server to reappear in the client list.
10. Reinstall the S-TAP. If you are using GIM to install the S-TAP, reinstall the S-TAP bundle with GIM and the following commands.

```
KTAP_ALLOW_COMBO=Y  
KTAP_LIVE_UPDATE=Y  
KTAP_ENABLED=Y
```

Partition error installing Guardium

If you receive a partition error, select Custom installation and specify the disk location and size explicitly.

Symptoms

When you install the Guardium appliance in VMWare, you receive the following error:

```
Error Partitioning  
Could not allocate requested partitions.  
Partitioning failed: Could not allocate partitions as primary partitions.  
Not enough space left to create partition for /boot.
```

Causes

When you install the Guardium system with VMWare, if you select Typical, VMWare uses configuration parameters that are predefined for the OS type in VMWare. These configuration parameters might not be suitable for this installation.

Environment

All Guardium configurations (collector, aggregator, central manager) are affected.

Resolving the problem

Select Custom installation and specify the disk location and size explicitly. Specify a disk size that is large enough for your monitoring and audit needs. After it is configured, Guardium does not support adding disk space to the system.

Patch installation fails: No such file or directory

If the patch installation fails, check that the file matches the MD5SUM of the downloaded patch.

Symptoms

Patch installation in Guardium fails with the error `patch.reg`:
`No such file or directory.`

Causes

The following cases can cause the patch installation to fail.

- The patch was not downloaded in binary mode and corrupted the file.
- The compressed file itself was uploaded to the Guardium system.
- The patch was received from Guardium support and has the PMR number prefixed to the file name.
- The patch was uploaded to the Guardium system from a Windows FTP server.

Environment

The collector, aggregator, and central manager are affected.

Resolving the problem

Verify that the contents of the file match the MD5SUM of the downloaded patch. If the compressed file cannot be extracted or the MD5SUM does not match, download the file in binary mode.

If the compressed file itself was uploaded to the Guardium system, extract the compressed file and upload only the patch.

If there is a PMR number prefixed to the file name, remove the number and then upload the patch to the Guardium system.

If the patch is uploaded from a Windows FTP server, specify the exact file name with the correct case.

z/OS

These sections present troubleshooting and solutions for common problems with z/OS.

- [z/OS S-TAP fails to show active the Guardium system](#)
If z/OS S-TAP fails to show active on the Guardium system, restart the inspection-core.

z/OS S-TAP fails to show active the Guardium system

If z/OS S-TAP fails to show active on the Guardium system, restart the inspection-core.

Symptoms

z/OS S-TAP fails to show active on the Guardium system after you start it for the first time. The policy is correctly configured with a DB2 or IMS Collection Profile and installed. The z/OS S-TAP is properly configured to use port 16022. All messages on the mainframe indicate connectivity.

Causes

If the collector has not been actively used as a collector since being built and configured, the sniffer appears to time out port 16022.

Environment

z/OS is affected.

Resolving the problem

Restart the inspection-core by using the CLI command `restart inspection-core`.

Guardium universal connector

Using the Guardium universal connector to work with other data sources.

The Guardium universal connector enables Guardium Data Protection and Guardium Insights to get data from potentially any data source's native activity logs without using the S-TAP.

You can access the documentation that is related to the Guardium Universal Connector as follows:

- [Developing new plug-ins for Guardium Data Protection](#)
- [Configuring the Guardium universal connector](#)
- [Configuring policies for the universal connector](#)
- [Monitoring connector and data flow status](#)
- [Troubleshooting Universal Connectors](#)
- [Guardium Universal Connector FAQs](#)
- [**Overview**](#)
Quick overview of the steps that are available to configure the Guardium universal connected end-to-end.
- [**Configuring policies for Universal connector**](#)
Policies for the Guardium universal connector are created and managed just like all other Guardium policies.
- [**Creating and managing secrets**](#)
Store secrets in the universal connector keystore to achieve higher security, instead of writing the passwords in plain text within a connector configuration. Store secrets before you add a connector configuration that is using a secret. Restart the universal connector to make the new or updated secrets available for universal connector configurations.
- [**Enabling universal connector on collectors**](#)
Enable the Guardium universal connector on collector by using the Guardium UI or by using the API commands.
- [**Adding connectors and plug-ins**](#)
The Guardium universal connector is the Guardium entry point for native audit logs. The Guardium universal connector identifies and parses the received events, and converts them to a standard Guardium format. The output of the Guardium universal connector is forwarded to the Guardium sniffer on the collector, for policy and auditing enforcements. Configure Guardium to read the native audit logs by customizing a pre-defined template for data sources that have pre-defined plug-ins (Amazon S3, MongoDB, and MySQL), or with your own plug-in.
- [**Universal connector configuration**](#)
12.1 and later You can centrally manage the Guardium® Managed Units where the Universal Connector is installed.
- [**Configuring universal connectors**](#)
Use the legacy Configure Universal Connector page on a Managed Unit to configure universal connectors.
- [**Monitoring connector and data flow status**](#)
The connectors are displayed in the standard Guardium reports and UI pages. You can check the general status of the connector by using the API or use the UI to view the status.
- [**Troubleshooting universal connectors**](#)
Use this page to systematically approach toward the solutions for the Universal Connector problems.

Overview

Quick overview of the steps that are available to configure the Guardium universal connected end-to-end.

Important: Your role must include S-TAP Management Application role permission.

1. Allocate Guardium collectors to receive the audit files.
2. For the data source types supported by Guardium, do the following.
 - a. Configure the native audit logs on the data source that Guardium can parse, and then configure the data shipper to forward the audit logs to the Guardium universal connector.
 - b. Configure the Guardium universal connector to read the native audit logs. For more information, see [Adding connectors and plug-ins](#) topic.
Note: If you are using secrets or sensitive information in the configuration, see [Creating and managing secrets](#) topic before you configure a new connector.
3. For a data source that does not have off-the-shelf support by Guardium, follow the instructions that are detailed in [upload a plug-in](#) topic.
4. Enable the universal collector feature on the designated Guardium collectors or the stand-alone system. For more information, see [Enabling universal connector on collectors](#) topic to enable the Guardium universal connector on collectors.

Configuring policies for Universal connector

Policies for the Guardium universal connector are created and managed just like all other Guardium policies.

The Guardium universal connector supports the following rule actions:

- Alert daily
- Alert only
- Alert per match
- Alert per time granularity
- Log full details
- Log full details with replaced values
- Log masked details
- Log only
- No parse (supported by connectors that use the sniffer parser to parse traffic.
For example, S3 and MongoDB plug-ins does not support this rule action. MySQL does support this rule action)
- Record values separately
- Quick parse (supported by connectors that use the sniffer parser to parse traffic.
For example, S3 and MongoDB plug-ins does not support this rule action. MySQL does support this rule action)
- Quick parse no fields (supported by connectors that use the sniffer parser to parse traffic.
For example, S3 and MongoDB plug-ins does not support this rule action. MySQL does support this rule action)

- Skip logging

For more information on actions, see [Actions](#).

Creating and managing secrets

Store secrets in the universal connector keystore to achieve higher security, instead of writing the passwords in plain text within a connector configuration. Store secrets before you add a connector configuration that is using a secret. Restart the universal connector to make the new or updated secrets available for universal connector configurations.

Procedure

1. Create a secret. Log in to the Guardium CLI and create the key by using the following grdapi command.

```
grdapi universal_connector_keystore_add key=<key_name> password=<key_value>
```

Note: Spaces are not allowed after and before = in this grdapi command.

2. Verify whether the keys are entered successfully by using the following command.

```
grdapi universal_connector_keystore_list
```

3. Add a key as an environment variable in the connector configuration.

a. Log in to Guardium and then go to the [Configure Universal Connector](#) page.

b. Upload jdbc driver (JAR file)

c. Add or edit a connector configuration to use a secret. Instead of writing the secret in plain text, type the key that you created as an environment variable.

For example:

```
jdbc { ... jdbc_connection_string => "jdbc:..." jdbc_user =>
"${MYSQL_USERX_NAME}" jdbc_password => "${MYSQL_USERX_PASSWORD}" ... }
      jdbc_password => "${MYSQL_USERX_PASSWORD}"
```

d. Save the configuration.

Note: To use the JDBC input plug-in, you need to upload a driver (JAR file) and then add the configuration.

4. To update a secret, you need to remove the key, add it again, and then restart the universal connector with overwriting old instance option.

a. To remove the key, run the following command.

```
grdapi universal_connector_keystore_remove key=<key_name>
```

b. To make sure that the key is no longer available to configurations, force the universal connector to fully restart, run the following command.

```
grdapi run_universal_connector overwrite_old_instance="true"
```

c. Listing the secret keys. To retrieve your updated list of the secrets after adding, removing, and updating keys, run the following command.

```
grdapi universal_connector_keystore_list
```

Enabling universal connector on collectors

Enable the Guardium universal connector on collector by using the Guardium UI or by using the API commands.

About this task

Tip: To simplify managing multiple collectors, create a managed unit group and use the API. For more information, see [Creating managed unit groups](#).

Attention: When you restart your Guardium system, restart the Guardium universal connector by using the following API command.

```
grdapi run_universal_connector
```

Procedure

1. On each collector that has connectors, enable the universal connector.

- For CLI, use the following commands:

```
grdapi run_universal_connector
```

To enable on multiple collectors by using the API, on the central manager enter.

```
grdapi run_universal_connector api_target_host=group:<managed unit group name>
```

- For Guardium UI, click **Setup** > **Tools** > **Tools and Views** > **Configure Universal Connector** and then click **Enable**.

2. Verify the connector status by using the following instructions.

- For CLI, use the following API command on managed unit.

```
grdapi get_universal_connector_status
```

- For Guardium UI: Verify that the **Disabled** option is active on the **Configure Universal Connector** page, which indicates that the Guardium Universal Connector is enabled.

Adding connectors and plug-ins

The Guardium universal connector is the Guardium entry point for native audit logs. The Guardium universal connector identifies and parses the received events, and converts them to a standard Guardium format. The output of the Guardium universal connector is forwarded to the Guardium sniffer on the collector, for policy and auditing enforcements. Configure Guardium to read the native audit logs by customizing a pre-defined template for data sources that have pre-defined plug-ins (Amazon S3, MongoDB, and MySQL), or with your own plug-in.

Before you begin

You must have permission for the role S-Tap Management. Admin user has this role by default.

About this task

Pre-defined plug-ins: Guardium has a few pre-defined plug-ins for specific data sources: Amazon S3, MongoDB, and MySQL. In this scenario, you do not need to upload a plug-in. Instead, you can use the corresponding template to help you to configure the input and the filter. The templates include all required fields. The input and filter sections conform to the sections in an Elastic Logstash configuration file, described [here](#).

The default MongoDB connector is the preferred method of ingesting data. It does not require any additional configuration on Guardium if you use the default configuration. By default, the Guardium universal connector listens for MongoDB audit log events that are sent over Syslog (TCP port 5000, UDP port 5141) and Filebeat (port 5044). If you cannot use these ports, or if a parameter does not display in the reports as you expect, update the MongoDB connector configuration to match your system.

Important: Each connector requires unique ports. Do not use the default ports for a customized connector configuration. Also, each connector must have a unique type, and the filter configuration must use that type.

For example, if the input configuration includes:

```
udp { port => 5141 type => "syslogMongoDB" }
```

then the filter must match it:

```
if [type] == "syslogMongoDB" {
```

Tip: When you save a connector configuration, Guardium stops the universal connector, verifies the new connection syntax, and initiates the new connection. Then, it restarts the universal connector. To prevent unnecessary loss of data during this stop period (usually about 1 minute), verify new configurations on a test Guardium system before you add them to your live system.

Procedure

1. On the collector, click **Setup** > **Tools and Views** > **Configure Universal Connector**.
2. Click the add icon.
3. For pre-defined plug-ins:
 - a. Enter name in the Connector name field.
 - b. From the Connector template drop-down list, select the template that most closely matches your system and follow the instructions in the sections that describe each template.
 - c. Click **Save**. Guardium validates the new connector, and enables the universal connector if it was disabled. After it is validated, it appears in the **Configure Universal Connector** page.
4. For offline plug-in package and related files, see further instructions in [upload a plug-in](#).

Universal connector configuration

12.1 and later You can centrally manage the Guardium® Managed Units where the Universal Connector is installed.

- By default, the option to centrally manage the Universal Connectors is enabled which automatically disables the traditional Configuring Universal Connector page.
- The traditional Configuring Universal Connector page is enabled only when you are upgrading to Guardium Data Protection version 12.1 and the Universal Connector data source is configured before the upgrade.
- If you are upgrading to Guardium Data Protection version 12.1, and you previously have not configured any universal connectors, the traditional Configure Universal Connector page is disabled. If you want to use the traditional Configure Universal Connector page to configure the Universal Connectors, use the grdapi modify_guard_param and update the LEGACY_UC_CONFIG_ENABLED parameter as follows:

```
grdapi modify_guard_param paramName=LEGACY_UC_CONFIG_ENABLED paramValue=1
```

- If you are upgrading to Guardium Data Protection version 12.1 and you have a Universal Connector that is enabled on a collector, use the traditional Configuring Universal Connector page to configure the Universal Connector. In this case, you cannot install the data source profiles by using the Central Manager until you manually delete the Universal Connector configurations on the collector and disable the traditional mode by using the GuardAPI modify_guard_param. To disable the traditional mode, update the LEGACY_UC_CONFIG_ENABLED parameter as follows:

```
grdapi modify_guard_param paramName=LEGACY_UC_CONFIG_ENABLED paramValue=0
```

Note: The `modify_guard_param` API is available with the Guardium Data Protection 12.1 version (fresh install) as well as Guardium Platform Upgrade flows.

- [**Creating credentials**](#)

12.1 and later Create, modify, delete, and refresh credentials for data sources such as JDBC, Google Cloud, AWS, and AWS Role ARN, which are used in the data source profiles.

- [**Creating data source profiles**](#)

12.1 and later Create a data source profile to configure Universal Connectors on Managed Units. You can also install, uninstall, reinstall the created profiles along with enabling, disabling, restarting, and troubleshooting Universal Connectors.

- [Creating Kafka clusters](#)
Create and manage the Kafka clusters for the data sources that require Kafka clusters.
- [Managing plug-ins](#)
12.1 and later Upload new plugins for the data sources that are not preinstalled on Guardium.

Related concepts

- [Creating credentials](#)

Related tasks

- [Creating data source profiles](#)
- [Creating Kafka clusters](#)
- [Managing plug-ins](#)

Creating credentials

12.1 and later Create, modify, delete, and refresh credentials for data sources such as JDBC, Google Cloud, AWS, and AWS Role ARN, which are used in the data source profiles.

Creating credentials

1. In Guardium Data Protection Central Manager, or standalone machine, click [Manage > Universal Connector > Credential Management](#).
2. To create new credentials, click the add  icon and enter the following details.

Table 1. Managing credential parameters

Parameters	Description
Name	Enter the name of the data source connection.
Description	Enter the data source description.
Credential type	Select one of the following credential types: <ul style="list-style-type: none"> • Google Cloud • JDBC • AWS • AWS Role ARN
• JDBC username and JDBC password • Service Account JSON key file • AWS access key ID and AWS secret access key • AWS Role ARN	Enter the details according to the type of credential that you selected.

Note: You can use the same credentials for multiple profiles.

The Credential Management table displays the credential details. When you hover over the Used in profile column, it displays the names of the data source profiles in which the credentials are used.

To search credentials by name, enter the credential name in the Filter field.

Creating data source profiles

12.1 and later Create a data source profile to configure Universal Connectors on Managed Units. You can also install, uninstall, reinstall the created profiles along with enabling, disabling, restarting, and troubleshooting Universal Connectors.

Procedure

1. In Guardium Data Protection Central Manager, or Standalone machine, click [Manage > Universal Connector > Datasource Profile Management](#).
2. To create a data source profile, click the add  icon and enter values in the following fields.

Table 1. Managing data source parameters

Parameters	Description
Name	Enter the name of the data source connection.
Description	Enter the data source description.
Plug-in	Select the plugin.
Credential	Enter the credentials that you created in the Credential Management page. To create new credentials, click the add  icon to create credentials. For more information, see Creating credentials . This field is displayed only if the plugin requires credentials.
Kafka cluster	Select the appropriate Kafka cluster from the available Kafka cluster list or to create a Kafka cluster, see Creating Kafka clusters . This field is displayed only if the plug-in requires the Kafka cluster.

Parameters	Description
Parameters <ul style="list-style-type: none"> • Maximum poll records • Poll timeout (milliseconds) 	Depending on the type of plug-in that is selected in the Plug-in field, enter the parameters value. For example, if you select Document DB over CloudWatch Logs plug-in, then see DocumentDB-Guardium Logstash filter plug-in . By default, the Maximum poll records value is 1000 and Poll timeout value is 500. To get more efficient results, you can increase the Kafka cluster partition by setting the Maximum poll record value as 2000. Restriction: Once you increase then partitions, they cannot be decreased. After you update the Maximum poll records value, reinstall the profile.
Initial Time (milliseconds)	The timestamp from which the connector starts polling for changes in the database. Setting this to 0 means the connector starts from the earliest available data. If used for incremental data fetching, this parameter ensures that only new data (after the initial time) is retrieved.
Hostname	Specifies the hostname or IP address of the Oracle database server. It is the address where the Oracle instance can be accessed for establishing a JDBC connection.
JDBC driver library	The Oracle JDBC driver JAR file (ojdbc8.jar) is required for the connector to communicate with the Oracle database. Download the Oracle JDBC driver JAR file and uploaded the driver to the Kafka Connect environment.
Port	Specifies the port number used to connect to the Oracle database. The default port number is 1521, but it can vary depending on the Oracle configuration. Port 1521 must be open and accessible for the connection.
Service Name / SID	Specifies the Oracle service name (or SID if it's an older configuration) for Kafka connector to connect. The service name uniquely identifies a database service within an Oracle environment and is provided by the database administrator

3. Click OK.
4. Select a profile, and select the relevant installation option from the Install list.
5. Click Actions and select one of the following applicable options:

Enable UC

Use this option to enable the UC on the applicable collectors.

Disable UC

Use this option to disable the UC on the applicable collectors.

Restart UC

Use this option to restart the UC on the applicable collectors.

Troubleshoot

Troubleshoots the collector for errors in the uc-logstash.log and logstash-plain.log file.

6. Click OK.
7. Download the server (data source) CA certificate to ensure that Syslog accepts the communication with data source.
 - a. Click Download server CA.
 - b. Copy the certificate to the database server and note the location. For more information, see [Installing an appliance certificate to avoid a browser SSL certificate challenge](#).

What to do next

If you have selected a plugin that requires a Kafka cluster, complete the following steps after creating the Kafka cluster and data source profile: [Configure native audit and rsyslog on Datasource Server](#).

Creating Kafka clusters

Create and manage the Kafka clusters for the data sources that require Kafka clusters.

Before you begin

Run the following command on the CLI to convert a new Managed Unit into a Kafka node.

```
store unit type kafka-node
```

Procedure

1. Click Manage > Universal Connector > Kafka Cluster Management.
2. Click the add  icon.
3. In the Name field, enter a unique cluster name.
4. To create a member in the Cluster member grid, click the add  icon.
5. From the Select units to add list, select the Kafka nodes, and click OK.
Note: Add at least three Kafka nodes in one cluster for equal load balancing.
6. Optional: If you want to authenticate database servers with the Kafka cluster, select Enable client authentication then upload a valid client certificate for each database server or a set of signing certificates to be used for validation of incoming connections.
7. Select one or more Kafka nodes from the Cluster member grid to create a Kafka cluster.
Expand the cluster and view the individual node Status and Details in the grid
8. Use the Start, Stop and Restart options to start, stop and restart the individual clusters.
Note: You can restart one or more nodes from a cluster
9. Download the server (Kafka cluster) CA certificate to ensure that syslog accepts the communication with Kafka cluster.
 - a. On the Kafka cluster management page, select a cluster from the grid and click Download server CA.
 - b. Copy the certificate to the database server and note the location. For more information, see [Installing an appliance certificate to avoid a browser SSL certificate challenge](#).

Results

The Kafka cluster is created successfully.

Note:

- To ensure no data failover and appropriate load balancing, define the same configuration name on the Managed Unit on all Universal Connectors in the same Kafka Cluster.
- You cannot direct data flow from different types of databases to the same Kafka cluster.

Related reference

- [get_kafka_clusters](#)
- [create_kafka_cluster](#)
- [delete_kafka_cluster](#)
- [edit_kafka_cluster](#)

Managing plug-ins

12.1 and later Upload new plugins for the data sources that are not preinstalled on Guardium.

About this task

By default, Guardium® Data Protection provides the following preinstalled plugins that you can use to create profiles.

- Aurora MySQL over CloudWatch Logs Input
- AWS MSSQL over JDBC
- Azure Postgres over Event Hub
- Dynamo over CloudWatch Logs
- Firebase over Google Pub/Sub
- MongoDB over Filebeat
- MySQL Over Filebeat
- OUA over JDBC connect
- Postgres over Kafka
- Postgres over SQS
- S3 over CloudWatch Logs

What to do next

Create a data source profile. For more information, see [Creating data source profiles](#).

Configuring universal connectors

Use the legacy Configure Universal Connector page on a Managed Unit to configure universal connectors.

About this task

Note: If you want to configure the Universal Connector using the new flow, then see [Universal connector configuration](#).

Restriction:

- If you upgrading to Guardium Data Protection version 12.1, and previously you have not configured any universal connectors on the Managed units, then in such case the Configure Universal Connector page is disabled. If you want to use Configure Universal Connector page to configure universal connectors then use the grdapapi modify_guard_param and update the LEGACY_UC_CONFIG_ENABLED as follows:

```
grdapapi modify_guard_param paramName=LEGACY_UC_CONFIG_ENABLED paramValue=1
```

Procedure

1. On the Collector, go to Setup > Tools and Views > Configure Universal Connector page.
2. Ensure that the Universal Connector is enabled.
3. To add a new configuration, click the add  icon.
4. Select the applicable connector template or use the .conf file from the GitHub repository. For example, see the [auroraMysqlCloudwatch.conf](#) file for Aurora-MySQL-Guardium Logstash filter plug-in.
Important: If you are configuring more than one filebeat connector on a single Managed Unit, then ensure to update the tags parameter in the filter plugin configuration file with unique values for each configuration. Not using unique values may affect the system performance.
5. In the Connector Name field, enter a unique connector name.
Ensure that the name does not contain special characters other than underscore(_) and hyphen (-).
6. Click Save.

Results

The Universal Connector is now configured and ready to receive new events from the data source.

Monitoring connector and data flow status

The connectors are displayed in the standard Guardium reports and UI pages. You can check the general status of the connector by using the API or use the UI to view the status.

Connector Status

The connectors display in the S-TAP pages of the UI only after data is received in the connector. Guardium creates the connector instance after data is received. If the connector does not have active traffic, then the connector does not display in the S-TAP Status or Events pages.

To verify that a new connector was configured successfully, and to see the connector status on the S-TAP status, run a test command on the data source and make sure you can see the new connector status.

You can typically see the connectors and their status in the following Guardium pages:

- S-TAP Status page. The connectors are indicated by using the following elements:
 - S-TAP Host - **database host: database port: UCn**.
 - S-TAP Version - **Universal connector Vn.n.n**.
 - Status - Indicates data flow by **Active** or **Inactive**.
- S-TAP Events
- Central manager pages:
 - In the Deployment Health Topology, click **Expand S-TAPs**. For more information, see [Deployment health topology and table views](#).
- In the Deployment Health Table, in the S-TAPs tab, you can identify connectors by
 - Under Hostname or IP address, the address ends in :UCn.
 - Under Version, the name is **Universal connector Vn.n.n..**

For details about the Deployment Health Table, see [Deployment health topology and table views](#).

- In the [Deployment health dashboard](#), S-TAPs by version chart, the Guardium universal connectors appear as S-TAPs with version numbers. In all other charts, the connectors are treated the same as S-TAPs.
- Enterprise S-TAP View to check S-TAP status. This report requires configuration. See [External data correlation][External data correlation](#)). Check for data flow in the Status column. The status Active indicates data flow.
- Detailed Enterprise S-TAP View. The Status column. The status Active indicates data flow. This report requires configuration. See [External data correlation][External data correlation](#)).

Note: If the universal connector displays in red, then it might be because of one of the following reasons:

- It was enabled, and then disabled.
- Data did not flow in over an hour.
- An issue occurred on the universal connector.

To view the connector status, run the following API command.

```
grdapi get_universal_connector_status
```

Data flow status

To view the data that is sent into Guardium, view the following pages.

- The connectors appear in many reports, similar to S-TAPs. Reports show data for connectors only if the connectors have policies that are installed, just like Guardium collectors. Make sure that you have a policy that is installed with the **Log Full Detail** rule action. Add reports to a dashboard, for example:
 - Full SQL (Clone and edit this report to test that other fields are inserted correctly into Guardium).
 - SQL Errors. You might need to add the description field to see your custom errors, if you pass a string to Guardium representing your custom error text.
 - Failed Login Attempts
- [Investigation dashboard](#). Data indexing is delayed by 2 minutes.

Restriction: An object that is deleted from a bucket is not specified in native audit events if the deletion was made from an S3 console. The delete operation appears in reports and the investigation dashboard, but the object name is not included.

- Set up Compliance Monitoring. For more information, see [Smart assistant for compliance monitoring](#). In the Database tab, you can identify data sources for monitoring.
- The Compliance monitoring page displays databases, if Guardium supports your DB and data is flowing into Guardium. This view updates once per hour, and displays databases that had remote activity in the past hour. You do not see anything here if you run commands directly from your DB server.

Troubleshooting universal connectors

Use this page to systematically approach toward the solutions for the Universal Connector problems.

- [Troubleshooting tool](#)

The troubleshooting tool helps you identify and resolve issues in UC connections. The troubleshooting tool scans your Logstash log files and searches for known

errors. Once it finds errors, it notifies you along with a description of the problem. Also, the troubleshooting tool checks the status of Sniffer and Squid services and informs you if either of them is inactive.

- [Logstash StackOverflow error due to large plug-in config file](#)

Troubleshooting tool

The troubleshooting tool helps you identify and resolve issues in UC connections. The troubleshooting tool scans your Logstash log files and searches for known errors. Once it finds errors, it notifies you along with a description of the problem. Also, the troubleshooting tool checks the status of Sniffer and Squid services and informs you if either of them is inactive.

About this task

To avoid old or irrelevant messages, the tool scans for errors in the Logstash logs file starting from the last time you ran troubleshooting. For example, if you last ran troubleshooting 3 hours ago, the troubleshooting tool will now only scan for errors from the past 3 hours. If this is your first time running the troubleshooting tool, it scans from the beginning of the Logstash logs file.

You can run the troubleshooting tool in the following 2 ways:

Restriction:

- The troubleshooting tool searches for errors starting from the last time you ran it. If you have not run the tool in a long time, it can take some time until new errors are observed and caught by the troubleshooting tool.
- The troubleshooting tool does not solve the issues. Rather, it gives you the relevant information about the root cause of the error so that you can fix it.

Procedure

1. Run the troubleshooting tool by using the following grasping.

```
grdapic universal_connector_troubleshooting
```

OR

2. Run the troubleshooting tool by using the Guardium Data Protection UI as follows.
Go to the Configure universal connector page and click Run troubleshooting.

Logstash StackOverflow error due to large plug-in config file

When you configure more than ten Universal Connectors on one collector, you might get the following StackOverflow error:

```
FATAL Logstash:109 - uncaught error (in thread Ruby-0-Thread-35: /usr/share/logstash/logstash-core/lib/logstash/java_pipeline.rb:289)
java.lang.StackOverflowError: null
    at org.logstash.config.ir.expression.EventValueExpression.toString(org/logstash/config/ir/expression/EventValueExpression.java:51)
~[logstash-core.jar:?]
    at java.lang.StringConcatHelper.stringOf(java/lang/StringConcatHelper.java:453) ~[?:?]
    at org.logstash.config.ir.expression.unaryTruthy.toRubyString(org/logstash/config/ir/expression/unary/Truthy.java:36) ~[logstash-core.jar:?]
    at org.logstash.config.ir.compiler.EventCondition$Compiler.buildCondition(org/logstash/config/ir/compiler/EventCondition.java:112)
~[logstash-core.jar:?]
    at org.logstash.config.ir.CompiledPipeline$CompiledExecution.lambda$compileDependencies$6(org/logstash/config/ir/CompiledPipeline.java:546) ~[logstash-core.jar:?]
    at java.util.stream.ReferencePipeline$3$1.accept(java/util/stream/ReferencePipeline.java:197) ~[?:?]
```

To avoid the stack overflow error, you can aggregate all connections and use one of the following optimized options.

Option 1

If you are configuring all the Universal Connectors from the same database type but different account IDs.
Consider the following existing workflow with three different connectors that have the same logic:

```
postgresql1:
  input { cloudwatch_logs { log_group=>"postgresql1", type=>"postgresql1" }
  filter {if type="postgresql1" {...} }

postgresql2:
  input { cloudwatch_logs { log_group=>"postgresql2", type=>"postgresql2" }
  filter {if type="postgresql2" {...} }

postgresql3:
  input { cloudwatch_logs { log_group=>"postgresql3", type=>"postgresql3" }
  filter {if type="postgresql3" {...} }
```

Following is the optimized workflow with 3 different connectors that have the same logic:

```
input {
  cloudwatch_logs { log_group=>"postgresql1", type=>"postgresql" }
  cloudwatch_logs { log_group=>"postgresql2", type=>"postgresql" }
  cloudwatch_logs { log_group=>"postgresql3", type=>"postgresql" }
```

```

}
filter {if type=="postgresql" {...} }

See the following example of CloudWatch plug-in config file with three different accounts, <ACCOUNT_ID_1>, <ACCOUNT_ID_2> and <ACCOUNT_ID_3>.

cloudwatch_logs {
log_group => ["<LOG_GROUP>"]
start_position => "end"
access_key_id => "<ACCESS_KEY_1>"
secret_access_key => "<SECRET_KEY_1>"
region => "<REGION_1>"
interval => 2
event_filter => ""
codec => multiline {
pattern => "((?<ts>[^A-Z]{3})*)UTC:(?<client_ip>[^:]*):(?<db_user>[@:]*)@(?<db_name>[^:]*):(?<session_id>[^:]*):(?  
<logger>LOCATION|DETAIL|STATEMENT|HINT):%{GREEDYDATA:sql_full_log})|(^s))"
negate => false
what => "previous"
}
type => "postgres"
add_field => {"account_id" => "<ACCOUNT_ID_1>"}
}


```

```

cloudwatch_logs {
log_group => ["<LOG_GROUP>"]
start_position => "end"
access_key_id => "<ACCESS_KEY_2>"
secret_access_key => "<SECRET_KEY_2>"
region => "<REGION_2>"
interval => 2
event_filter => ""
codec => multiline {
pattern => "((?<ts>[^A-Z]{3})*)UTC:(?<client_ip>[^:]*):(?<db_user>[@:]*)@(?<db_name>[^:]*):(?<session_id>[^:]*):(?  
<logger>LOCATION|DETAIL|STATEMENT|HINT):%{GREEDYDATA:sql_full_log})|(^s))" negate => false
what => "previous"
}
type => "postgres"
add_field => {"account_id" => "<ACCOUNT_ID_2>"}
}


```

```

cloudwatch_logs {
log_group => ["<LOG_GROUP>"]
start_position => "end"
access_key_id => "<ACCESS_KEY_3>"
secret_access_key => "<SECRET_KEY_3>"
region => "<REGION_3>"
interval => 2
event_filter => ""
codec => multiline {
pattern => "((?<ts>[^A-Z]{3})*)UTC:(?<client_ip>[^:]*):(?<db_user>[@:]*)@(?<db_name>[^:]*):(?<session_id>[^:]*):(?  
<logger>LOCATION|DETAIL|STATEMENT|HINT):%{GREEDYDATA:sql_full_log})|(^s))" negate => false
what => "previous"
}
type => "postgres"
add_field => {"account_id" => "<ACCOUNT_ID_3>"}
}


```

Options 2

If you are configuring all the Universal Connectors from the same database type, within the same database account and with same account ID. Consider the following existing workflow with three different connectors that have the same logic:

```

postgresql1:
input { cloudwatch_logs { log_group=>"postgresql1", type=>"postgresql1" }
filter {if type=="postgresql1" {...} }

postgresql2:
input { cloudwatch_logs { log_group=>"postgresql2", type=>"postgresql2" }
filter {if type=="postgresql2" {...} }

postgresql3:
input { cloudwatch_logs { log_group=>"postgresql3", type=>"postgresql3" }

filter {if type=="postgresql2" {...} }


```

Following is the optimized workflow with 3 different connectors that have the same logic:

```

input { cloudwatch_logs { log_group=>"postgresql1, postgresql2, postgresql3", type=>"postgresql" }
filter {if type=="postgresql" {...} }


```

See the following example of CloudWatch plug-in config file with same account ID.

```

cloudwatch_logs {
log_group => ["<LOG_GROUP_1>", <LOG_GROUP_2>, <LOG_GROUP_3>]
#e.g. [/aws/rds/instance/database-1/postgresql1, /aws/rds/instance/database-2/postgresql1, /aws/rds/instance/database-  
3/postgresql1]
start_position => "end"
access_key_id => "<ACCESS_KEY>"
secret_access_key => "<SECRET_KEY>"
region => "<REGION>"
interval => 2
event_filter => ""
codec => multiline {


```

```

pattern => "((({<ts>[^A-Z]{3}}*)UTC:({<client_ip>[^:]*) : ({<db_user>[^@]*)@({<db_name>[^:]*) : ({<session_id>[^:]*) : (?
<logger>LOCATION|DETAIL|STATEMENT|HINT}:{%{GREEDYDATA:sql_full_log}}|(^s))"
negate => false
what => "previous"
}
type => "postgres"
add_field => {"account_id" => "<ACCOUNT_ID>"}
}

```

Windows: S-TAP user's guide

The Guardium S-TAP is a lightweight software agent installed on database servers and file servers. The S-TAP generally accounts for between 1% - 3% of CPU usage. In most installations, the impact is negligible with no noticeable impact on performance. The information collected by the S-TAPs is the basis of all Guardium traffic reports, alerts, visualizations, etc.

For data activity monitoring, the S-TAP monitors activity between the client and the database and forwards that information to the Guardium collector. The database traffic is logged into the collector based on criteria specified in the security policy. You can reduce the amount of traffic that is originally sent to the collector by ignoring trusted connections or ignoring traffic from specific IPs.

MySQL limitations: For MySQL, TCP is the only supported protocol. In addition, Windows S-TAP does not support MySQL encrypted traffic.

- [Windows: S-TAP authentication guidelines](#)
Most the S-TAP services run under a standard nonprivileged user account. Learn about this account, and the Guardium Services group.
- [Windows: S-TAP protocol 8](#)
The new S-TAP protocol 8 reduces CPU usage and memory usage. The two S-TAP protocols co-exist and use the same guard_tap.ini configuration file. You choose which protocol you want to use for each S-TAP.
- [Windows: Install, upgrade, and uninstall the S-TAP agent](#)
You can install, upgrade, and uninstall S-TAPs by using a few methods. Learn about each one and understand what works best for you.
- [Windows: Configuring S-TAP](#)
Learn to configure the S-TAP.
- [Windows: S-TAP configuration per database type](#)
This section provides detailed instructions or examples for configuring monitoring on various databases.
- [Windows: S-TAP operation and performance](#)
- [Windows: Scheduling S-TAP diagnostics](#)
You can schedule S-TAP diagnostics by using the S-TAP Diagnostic Scheduler user interface.

Windows: S-TAP authentication guidelines

Most the S-TAP services run under a standard nonprivileged user account. Learn about this account, and the Guardium Services group.

During a typical, fresh installation, the majority of the S-TAP services are installed under the Local Service account by default, except for GIM, FAM for NAS/SP and FDEC for NAS/SP services, which default to Local System.

During a fresh, custom, install users can select the custom account of their choice, including standard, nonprivileged, user accounts.

Upgrades continue to use whatever service account was in place at the time of the fresh install with one important exception. Services that run under Local System (except for GIM and NAS/SP) are converted to run under Local Service during an upgrade to one of V10.6.0.178, V11.0.1.x, and V11.1.0.x and higher. This effectively transitions an installation to run under a standard user account rather than an account with full privileges. If the original fresh installation used a custom account, you can remove that account from all privileged groups (like Administrators) after the upgrade.

The focal point of all S-TAP security checks is a local group named "Guardium Services" that are created during installation. The service account selected for the Guardium services by the user, whether it be Local Service or some custom account, is added as a member to the Guardium Services group. All service, file, and registry access are then granted to the Guardium Services group on behalf of those services, files, and registry keys that the Guardium services must access and control. If the system administrator manually changes the service account for the Guardium services at a later date, the new account must be manually added into the local system's Guardium Services group as a member.

The Guardium Services group grants only those privileges that are required to the services that require them. In most cases, there are no special requirements and the services run completely non-privileged. The Guardium Database Monitor service and the DB2 Tap service must, however, be granted the privilege **SeDebugPrivilege**.

Windows: S-TAP protocol 8

The new S-TAP protocol 8 reduces CPU usage and memory usage. The two S-TAP protocols co-exist and use the same guard_tap.ini configuration file. You choose which protocol you want to use for each S-TAP.

Changes include,

- New parameters in the guard_tap.ini configuration file. Some of the protocol 7 parameters are not valid for protocol 8. See all parameters, new and old, in [Editing the protocol 8 S-TAP configuration parameters](#).
- [Windows: Multi-threading S-TAP for increased throughput](#).
- Logging is saved in a circular text log. See [Windows: Log and debug files](#).
- Choose your S-TAP protocol by using the GIM parameter WINSTAP_V8_PROTOCOL, or the guard_tap.ini parameter V8_PROTOCOL, where:
 - 0 - Disabled (protocol 7)
 - 1 - Enabled (protocol 8)
- See [General parameters](#) and [Protocol 8 General parameters](#).

Windows: Install, upgrade, and uninstall the S-TAP agent

You can install, upgrade, and uninstall S-TAPs by using a few methods. Learn about each one and understand what works best for you.

The Base Filtering Engine (BFE) service must be running for the S-TAP installation. If the service exists but is not running, Guardium attempts to start it.

S-TAPs require .NET Framework 4.5 or higher version. If the .NET 4.5 or higher environment does not exist, S-TAP installs .NET 4.5.2.

All files and directories under Windows S-TAP and all Guardium® Windows agents installed directories give full control permission to the *Guardium Services* group. Guardium agents are designed so that Guardium creates the *Guardium Services* group the first time that you install Windows S-TAP or any other Guardium Windows agent.

S-TAP installation creates one installation log called `C:\IBM Windows S-TAP.ctl`.

The Windows S-TAP can be uninstalled without restarting. Upgrade your S-TAP to 11.4 (or later), reboot the S-TAP once, for example, in the next maintenance window. Then, you can uninstall the S-TAP without rebooting the database server or restarting database instances. A fresh install of the 11.4 (or later) S-TAP out of the box is fully uninstallable without requiring a reboot. Db2® exit monitoring requires a one time stop of the Db2 instances to install the Guardium interface DLL. After that, the S-TAP can be installed and uninstalled without stopping any instances.

Enterprise load balancing

During installation of an S-TAP on Windows, you can configure the S-TAP to use Enterprise Load Balancing features. For more information, see [Enterprise Load Balancing](#).

- [Windows: Install S-TAP agents installation flow](#)

Verify prerequisites, then install an S-TAP on Windows servers using the Deploy Monitoring Agents tool, the Guardium Installation Manager (GIM), the wizard, or the command line interface (CLI).

- [Windows: S-TAP monitoring mechanisms support matrix](#)

Select your S-TAP setup depending on the data that you want to monitor or block. Use this table to identify the monitoring mechanisms that can perform the operations that you require, per operating system and database.

- [Windows: Auto discovery of database instances during installation and upgrade](#)

When you install an S-TAP, it can auto-discover database instances and create inspection engines for the discovered instances.

- [Windows: Prerequisites: Installing S-TAP](#)

Review the disk space and port prerequisites before installing S-TAP:

- [Windows: Use GIM to install, upgrade, uninstall the S-TAP](#)

Use GIM Setup by Client to manage your S-TAPs.

- [Windows: Use interactive installer \(wizard\) to install, upgrade, uninstall the S-TAP](#)

- [Windows: Use CLI to install, upgrade, uninstall the S-TAP](#)

- [Windows: Remove the S-TAP using Add/Remove Programs](#)

You can use Add/Remove Programs to uninstall S-TAP no matter how it was installed. (For GIM installs, best practice ie to uninstall with GIM.)

- [Windows: S-TAP installation flow on Oracle RAC](#)

Configure S-TAPs in an Oracle RAC.

- [Windows: Managing S-TAP when upgrading your database](#)

Use these guidelines for managing your Windows S-TAP when upgrading your database.

- [Windows: Managing S-TAP when upgrading your database operating system](#)

Use these guidelines for managing an S-TAP, when upgrading the operating system (OS) of your database. This is relevant for all S-TAPs, regardless of the installation method.

- [Windows: When to restart or reboot the database server after installing or upgrading S-TAP](#)

In general, you do not need to reboot the database server after you install or upgrade Windows S-TAP unless you are upgrading between versions or when stated otherwise in the release notes.

Related concepts

- [Deploy monitoring agents](#)
- [Guardium Installation Manager](#)

Windows: Install S-TAP agents installation flow

Verify prerequisites, then install an S-TAP on Windows servers using the Deploy Monitoring Agents tool, the Guardium Installation Manager (GIM), the wizard, or the command line interface (CLI).

Depending on your license key, you can use the same S-TAP agent for both file server and database activity monitoring. FAM does not require any specific S-TAP configuration.

This flow describes installing S-TAP on a single database reporting to one collector.

1. Plan the installation, review these topics:

- [Windows: S-TAP monitoring mechanisms support matrix](#)
- [Windows: Auto discovery of database instances during installation and upgrade](#)
- [Windows: Discover database instances](#)

2. Verify the prerequisites.

- [Windows: S-TAP disk space requirements](#)
- [Windows: Guardium port requirements for S-TAP](#)
- If you are installing with GIM, the GIM client must be installed on the target database server. See [Installing the GIM client on a Windows server](#).

3. Install the S-TAP by one of:

- [Deploy monitoring agents](#)
- [Windows: Use GIM to install, upgrade, uninstall the S-TAP](#)
- [Windows: Use interactive installer \(wizard\) to install, upgrade, uninstall the S-TAP](#)

- [Windows: Use CLI to install, upgrade, uninstall the S-TAP](#)

During S-TAP installation, if auto-discovery is enabled, it auto-discovers databases and creates inspection engines for the discovered databases. The auto-discovery process runs once at the time of S-TAP installation and does not automatically repeat. Post-installation, it runs periodically and sends the details to the primary (current active) S-TAP host. You can modify the configuration after the installation is complete.

4. Configure any of the optional components if required by your system.

- [Windows: S-TAP installation flow on Oracle RAC](#)
- [Windows: Configuring the Db2 Exit library](#)
- [Windows: S-TAP load balancing models and configuration guidelines](#)

5. Reboot or restart if required ([Windows: When to restart or reboot the database server after installing or upgrading S-TAP](#)).

6. Complete the S-TAP configuration.

- [Configuring S-TAP in the S-TAP Control page](#)
- Advanced users only: [Editing the protocol 7 and protocol 8 S-TAP configuration parameters](#) and [Editing the protocol 8 S-TAP configuration parameters](#)

7. If required, configure [Enterprise Load Balancing](#).

Windows: S-TAP monitoring mechanisms support matrix

Select your S-TAP setup depending on the data that you want to monitor or block. Use this table to identify the monitoring mechanisms that can perform the operations that you require, per operating system and database.

For example, you might want to track the following information or perform one of the following procedures:

- Local traffic only
- Local and network traffic
- Shared memory
- Encrypted data
- Monitor and block
- Monitor only

The [Guardium support matrix](#) covers the most common platforms, database types, and protocols supported by Guardium monitoring mechanisms. The table presents general guidelines. Other combinations that are not presented here might be supported. Some of the supported setups that are shown here might depend on specific configurations. Contact Technical Support to verify the best setup for your specific needs. Empty cells indicate that the combination is not supported.

Windows: Auto discovery of database instances during installation and upgrade

When you install an S-TAP, it can auto-discover database instances and create inspection engines for the discovered instances.

By default, auto discovery runs once during S-TAP installation. It discovers the database instances, populates inspection engines according to its discovery, and updates the S-TAP configuration file guard_tap.ini. When the installation is complete, auto discovery is disabled to prevent the S-TAP from overwriting user-modified inspection engine configurations. The Guardium® Discovery Agent is installed with the S-TAP package on a database server.

Auto discovery is controlled by the guard_tap.ini parameter AUTO_DISCOVERY. For more information, see [Discovery parameters](#) or [Protocol 8 Discovery parameters](#).

During an upgrade, auto-discovery identifies new database instances but does not create inspection engines for the new instances.

CAUTION:

If you enable auto-discovery before upgrading the S-TAP, then **all** inspection engines are updated according to the discovered instances. If you changed the port range, for example, it reverts during the upgrade if auto discovery is enabled.

If you want to retain the inspection engine configurations, disable auto discovery before the upgrade.

All Windows S-TAP database types are supported for auto-discovery.

The auto discovery parameters should be left at their default values, except for advanced users. Discovery also uses these parameters:

- software_tap_host: IP address or hostname of the database server on which the S-TAP is installed.
- sqlguard_ip: S-TAP discovery results are sent to this IP. (The Guardium system with primary=1 in the SQLguard parameters.)

Instance discovery is configured and run independently of auto discovery. For more information, see [Windows: Discover database instances](#).

Windows: Prerequisites: Installing S-TAP

Review the disk space and port prerequisites before installing S-TAP:

- [Windows: S-TAP disk space requirements](#)

Verify the disk space requirements before installing your S-TAP.

- [Windows: Guardium port requirements for S-TAP](#)

If there is a firewall between Guardium® components (for example, between a Guardium system and an S-TAP on a Windows database server), you must verify that the ports used for connections between those components are not being blocked.

Windows: S-TAP disk space requirements

Verify the disk space requirements before installing your S-TAP.

Disk Space	Description
------------	-------------

Disk Space	Description
S-TAP program files	S-TAP uses the Microsoft .NET Framework. If this is not already installed, it requires 5GB free space GIM Install: 300 MB non-GIM Install: 180 MB
Buffer file	50 MB

Windows: Guardium port requirements for S-TAP

If there is a firewall between Guardium® components (for example, between a Guardium system and an S-TAP on a Windows database server), you must verify that the ports used for connections between those components are not being blocked.

Use your firewall management utility to check, and open as relevant, the ports listed below.

Table 1. Port Requirements for Windows servers

Port	Protocol	Guardium system connection to ...
9500/9501	TCP	Alive messages for S-TAP using Protocol 7
9800/9801	TCP	Alive messages for S-TAP using Protocol 8
9500	TCP	Clear S-TAP
9501	TLS	Encrypted S-TAP

Windows: Use GIM to install, upgrade, uninstall the S-TAP

Use GIM Setup by Client to manage your S-TAPs.

- [Windows: Installing S-TAP agent with GIM Setup by Client](#)

When you install S-TAPs on your database servers with the GIM Setup by Client, you can install, upgrade, and manage agents on individual servers or groups of servers. This includes monitoring processes that were installed under its control, modifying S-TAP parameters, and performing other management tasks.

- [Windows: S-TAP GIM installation parameters](#)

Understand the parameters (each with a short description) that are typically used in your GIM installation.

- [Windows: Upgrading S-TAP agent with GIM Setup by Client](#)

- [Windows: Uninstalling an S-TAP agent with GIM Set up by Client](#)

Learn how to uninstall the S-TAP agent and the GIM bundle from the database server. If S-TAP was installed with GIM, uninstall it with GIM. Otherwise, you need to manually remove the S-TAP folder from the GIM directory on the DB server.

Windows: Installing S-TAP agent with GIM Setup by Client

When you install S-TAPs on your database servers with the GIM Setup by Client, you can install, upgrade, and manage agents on individual servers or groups of servers. This includes monitoring processes that were installed under its control, modifying S-TAP parameters, and performing other management tasks.

Before you begin

Verify the following before you begin:

- Review the Windows S-TAP installation requirements at [Windows: Prerequisites: Installing S-TAP](#).
- Your database server and operating system are supported.
- The intended S-TAP installation directory is empty or does not exist.
- The GIM client is installed on the database server where you will install an S-TAP.
- The GIM client on the database server is communicating with the Guardium system. (Look for the client IP in Manage > Module Installation > GIM Processes Monitor.)
- Obtain the S-TAP module from either [Fix Central](#), or your Guardium representative.

About this task

After installing a GIM client on the database server, installation of the S-TAP for Windows is scheduled from the Guardium system.

The only required parameter is WINSTAP_INSTALL_DIR. It cannot be modified after the installation. All other parameters can be modified after installation.

You can input any parameter in the Setup by Client page, in the Choose parameters row, using the command WINSTAP_CMD_LINE with the syntax **parameter=value** for [TAP] parameters, or with the syntax **-param value** for CLI parameters ([Windows: S-TAP command line installation parameters](#)), and they are added or updated in the file guard_tap.ini.

CAUTION:

There is no validation of input when using the WINSTAP_CMD_LINE.

Procedure

1. Upload the Windows S-TAP module for installation.
 - a. On the Guardium® system, navigate to Manage > Module Installation > Upload Modules.

- b. Click Choose File and select the S-TAP module you want to install.
 - c. Click Upload to upload the module to the Guardium system.
After uploading, the module is listed in the Import Uploaded Modules table.
 - d. In the Import Uploaded Modules table, click the check box next to the S-TAP module you want to install.
The module is imported and made available for installation. After the module is imported, the Upload Modules page is reset and the Import Uploaded Modules table is empty.
2. Follow the GIM instructions in [Set up by Client](#) and refer to [Windows: S-TAP GIM installation parameters](#).
- While the default parameters are acceptable for most installations, you are required to provide a WINSTAP_INSTALL_DIR value. The default value is C:/Program Files/IBM/Windows S-TAP. This is the only required parameter.
 - If WINSTAP_TAP_IP (equivalent to the -taphost command line parameter) is not specified, the GIM_CLIENT_IP value is used.
 - If WINSTAP_SQLGUARD_IP (equivalent to the -appliance command line parameter) is not specified, the GIM_URL value is used.
 - Optionally enable enterprise load balancing. See the parameter description in [Windows: S-TAP GIM installation parameters](#).
 - If you want to disable auto-discovery, set WINSTAP_AUTO_DISCOVERY=0. For more information, see [Windows: Auto discovery of database instances during installation and upgrade](#).

What to do next

In the Success popup, click Show Status to open the Status window to monitor the software install/upgrade. Click  to refresh the results. If an install/upgrade has a failed status, click Uninstall if you see the button, otherwise, click Reset connection. You can also view the status of the module installation by reviewing the report at Manage > Reports > Install Management > GIM Clients Status.

Verify that the S-TAP is communicating with the Guardium system by browsing to Manage > Activity Monitoring > S-TAP Control and reviewing the S-TAPs status and configuration.

Related concepts

- [Guardium Installation Manager](#)

Windows: S-TAP GIM installation parameters

Understand the parameters (each with a short description) that are typically used in your GIM installation.

Depending on which protocol you are using, parameters are listed in either [Editing the protocol 7 and protocol 8 S-TAP configuration parameters](#) or [Editing the protocol 8 S-TAP configuration parameters](#).

CAUTION:

Do not modify advanced parameters unless you are an expert user or you are consulting with IBM Technical Support.

Attention: If a parameter is available through both the GIM and the command line interface (CLI), then the GIM parameter, including any defaults, always overwrites any value that is available from **WINSTAP_CMD_LINE**.

Table 1. Parameters applicable to all .NET installers

GIM parameter	Description
QUIET	Install silently. (Does not require value)
WINSTAP_INSTALL_DIR	The installation directory. The default installation path is C:\Program Files\IBM\Windows S-TAP

Table 2. Other S-TAP parameters

GIM parameter	Description
WINSTAP_AUTO_DISCOVERY	Controls auto-discovery of database instances. When enabled during installation, the agent discovers database instances on the server, populates inspection engines, and updates the guard_tap.ini configuration files. The parameter value is 1 during a fresh installation and changes to 0 after the initial installation. For more information, see Windows: Auto discovery of database instances during installation and upgrade . Valid values: <ul style="list-style-type: none"> • 0: disable • 1: enable
WINSTAP_ENABLED	Enables or disables S-TAP and its services. Default is enabled (1).
WINSTAP_ENABLE_GAM	Enables the Guardium Agent Monitor service (GAM). Default is disabled (0).
WINSTAP_INSTALLER_LOG_DIR	Specifies the location for storing the S-TAP installer log files. Use this parameter if you don't want to use the default location (C:).
WINSTAP_SQLGUARD_IP	The SQLGUARD IP. You can set up multiple appliances by specifying this parameter multiple times, each with a unique value.
WINSTAP_TAP_IP	The local/client IP. Required for unattended installation.

Table 3. S-TAP parameters that default to ON. The following parameters are set to either ON or 1 for some parameters by default. Setting these parameters to any value other than ON or 1 disables the parameter.

GIM parameter	Description
WINSTAP_TCP_DRIVER_INSTALLED	To use the TCP driver, set WINSTAP_TCP_DRIVER_INSTALLED=1 (the default). To disable the TCP driver, set this parameter to 0.

GIM parameter	Description
WINSTAP_NAMED_PIPE_DRIVER_INSTALLED	To use the named pipe driver, set NAMED_PIPE_DRIVER_INSTALLED=1 (the default). Specifies the named pipe that is used by MS SQL Server for local access. If a named pipe is used, but nothing is specified in this parameter, S-TAP attempts to retrieve the named pipe name from the registry. In rare cases, the S-TAP named pipes driver can interact with other third-party software in ways that slow the server down. To turn off the named pipes driver, set this parameter to 0. The named pipes driver is removed at the next system reboot. Note: If you turn off the named pipes driver, then the S-TAP does not capture named pipes traffic.
WINSTAP_DB2_TAP_INSTALLED	Enables sniffing Db2 shared memory traffic.
WINSTAP_DB2_EXIT_DRIVER_INSTALLED	Enables Db2 Integration with S-TAP.
WINSTAP_ORA_DRIVER_INSTALLED	Enables sniffing Oracle ASO and SSL traffic.

Table 4. Enterprise load-balancing parameters. For more information, see [Enterprise load balancing](#).

GIM parameter	Description
WINSTAP_LOAD_BALANCE_R_IP	Required if you are configuring enterprise load balancing. If blank, enterprise load balancing is disabled. The IP address or hostname of the central manager or managed unit this S-TAP uses for load balancing. Dynamic parameter. When you modify the value in the guard_tap.ini, you do not need to restart the S-TAP for the updated values to take effect.
WINSTAP_INITIAL_BALANCER_TAP_GROUP	The name of the S-TAP group that this S-TAP belongs to, for enterprise load balancing.
WINSTAP_INITIAL_BALANCER_MU_GROUP	The name of the managed unit group that the app-group is associated with. Requires a defined LB-APP-GROUP. The managed unit group must exist on the central manager before it can be used during installation of the S-TAP.
WINSTAP_LOAD_BALANCE_R_NUM_MUS	The number of managed units the enterprise load balancer allocates for this S-TAP.

Note: S-TAP parameters cannot be changed via the interactive installer during upgrade. After you upgrade, you can change S-TAP parameters either from the Guardium UI or by using the [update_stap_config](#) API.

Related tasks

- [Set up by Client](#)

Related reference

- [update_stap_config](#)

Windows: Upgrading S-TAP agent with GIM Setup by Client

Before you begin

Verify the following before you begin:

- Review the Windows S-TAP installation requirements at [Windows: Prerequisites: Installing S-TAP](#).
- Obtain the S-TAP module from either [Fix Central](#), or your Guardium representative.

Note: **Db2 servers.** When upgrading an S-TAP from 11.3 or before to 11.4 or later on Db2 servers, the S-TAP cannot continue to capture the Db2 server traffic. Stop and restart your Db2 instances after the S-TAP upgrade to resume capturing Db2 traffic. Subsequent upgrades do not require you to restart the instances.

Important: When you upgrade Windows S-TAP from 10.x to 11.x (or newer) using GIM, the FIREWALL properties are reset to the default values. Set WINSTAP_FIREWALL_INSTALLED=1 during the upgrade if you are using the firewall (S-GATE).

Procedure

1. Upload the Windows S-TAP module for upgrade.
 - a. On the Guardium® system, go to **Manage > Module Installation > Upload Modules**.
 - b. Click Choose File and select the S-TAP module you want to install.
 - c. Click Upload to upload the module to the Guardium system.

After uploading, the module is listed in the Import Uploaded Modules table.

 - d. In the Import Uploaded Modules table, click the check box next to the S-TAP module you want to install.

The module is imported and made available for upgrade. After the module is imported, the Upload Modules page is reset and the Import Uploaded Modules table is empty.
2. Go to **Manage > Module Installation > Set up by Client**.
3. In the Choose clients section, select the database servers where you want to update software. Select individual clients using check boxes in the table, or use the Select client group menu to select a group of clients.
Click Next to continue.
4. In the Choose bundle section, use the Select a bundle menu to identify your upgrade version. Click Next to continue.
5. If you are upgrading from 10.x to 11.0 (or newer), and you use the firewall: In the Choose parameters section, set WINSTAP_FIREWALL_INSTALLED to 1.
6. Click Install to begin the software upgrade. Or use the  icon to schedule the installation, then click OK to continue.
7. To create the Guardium API syntax for the current configuration in the Setup by Client, click Generate GuardAPI. If enough information is available, it generates API commands for multiple clients in the GuardAPI commands dialog. If there isn't enough information, it shows a default template.

What to do next

In the Success popup, click Show Status to open the Status window to monitor the software install/upgrade. Click  to refresh the results. If an upgrade has a failed status, click Uninstall if you see the button, otherwise, click Reset connection. You can also view the status of the module installation by reviewing the report at Manage > Reports > Install Management > GIM Clients Status.

If you see a Failed installation status for a bundle or module, open the Choose bundle section, select the client, click Uninstall, and use the  icon to monitor the installation status. If Uninstall is not available, open the Choose clients panel, select the affected client, and click Reset connection. Use the  icon to monitor the client list as the connection is reset.

Verify that the S-TAP is communicating with the Guardium system by browsing to Manage > Activity Monitoring > S-TAP Control and reviewing the S-TAPs status and configuration.

Related concepts

- [Guardium Installation Manager](#)

Related tasks

- [Set up by Client](#)

Related reference

- [Windows: S-TAP GIM installation parameters](#)

Windows: Uninstalling an S-TAP agent with GIM Set up by Client

Learn how to uninstall the S-TAP agent and the GIM bundle from the database server. If S-TAP was installed with GIM, uninstall it with GIM. Otherwise, you need to manually remove the S-TAP folder from the GIM directory on the DB server.

Before you begin

About this task

The Windows S-TAP can be uninstalled without reboot. Upgrade your S-TAP to 11.4 or later, reboot the S-TAP once, for example, in the next maintenance window. Then, you can uninstall the S-TAP without rebooting the database server or restarting database instances. A fresh install of the 11.4 or later S-TAP out of the box is fully uninstallable without requiring a reboot.

Procedure

1. Go to Manage > Module Installation > Set up by Client.
2. In the Choose clients section, select the database servers from which you are uninstalling the S-TAP. Select individual clients using check boxes in the table, or use the Select client group menu to select a group of clients. Click Next to continue.
3. In the Choose bundle section, select the bundle that you want to uninstall from the drop-down list.
Tip:
 - You can filter the clients, for example, by name, module, Selected bundle actions, and client OS. The resulting selection is persistent; **the action is applied only to the filtered list of clients**. You can see that the number of clients in the Choose Clients section is greater than the number in Configure Clients section.
 - Clear the Show only latest versions checkbox to view and work with earlier versions of a bundle.
 - Clear the Show only bundles checkbox to identify individual modules within a bundle.
 - Select the Show only compatible clients checkbox to hide clients that are not compatible with the selected bundle.The Configure Clients row shows the number of clients that have that specific bundle running. Click Next to continue.
4. Click Uninstall. The system prompts for confirmation. Click Yes.

Related concepts

- [Guardium Installation Manager](#)

Windows: Use interactive installer (wizard) to install, upgrade, uninstall the S-TAP

- [Windows: Installing S-TAP agent by using the interactive installer](#)

The interactive installer is useful for smaller deployments or whenever a guided, step-by-step installation experience is required.

- [Windows: Upgrading the S-TAP agent using the interactive installer](#)

The interactive installer is useful for smaller deployments or whenever a guided, step-by-step installation experience is required.

Windows: Installing S-TAP agent by using the interactive installer

The interactive installer is useful for smaller deployments or whenever a guided, step-by-step installation experience is required.

Before you begin

Verify the following before you begin:

- Review the Windows S-TAP installation requirements at [Windows: Prerequisites: Installing S-TAP](#).
- Verify that your database server and operating system are supported. For more information, see [System requirements](#) and the [Windows: S-TAP monitoring mechanisms support matrix](#).
- Identify the IP address of the database server where you are installing the S-TAP, including any virtual IP addresses.
- Identify the IP address of the Guardium® system that will control the S-TAP.
- Verify that the intended S-TAP installation directory is empty or does not exist.
- Obtain the S-TAP module from either [Fix Central](#), or from your Guardium representative.

About this task

When you install an S-TAP on a database server, you must provide the IP address or host name of the Guardium system that will receive data from the S-TAP. After the S-TAP has connected to the Guardium system, go to the [Manage > Activity Monitoring > S-TAP Control](#) page and complete the S-TAP configuration.

If you want to disable auto-discovery, clear the Start S-Tap Service checkbox. For more information, see [Windows: Auto discovery of database instances during installation and upgrade](#).

- You can change some Windows S-TAP parameters from the interactive installer (but not all). Use the GUI after you install the S-TAP to change S-TAP parameters that you can't change from the installer.

Note: You cannot install or run Windows S-TAP on a domain controller.

When you install an S-TAP from the wizard, you can uninstall it from the wizard, the command line, or Windows Add/Remove Programs.

Procedure

1. Log on to the database server with a system administrator account.
2. Copy the S-TAP module to your database and start the Guardium Windows S-TAP Install Wizard.
Attention: To install an S-TAP on Windows 2012 or later, you must use administrative privileges. Right-click the installer and choose Run as Administrator.
3. Read the license agreement on the Guardium License screen. To continue installation, select I accept the terms of the license agreement and click Next.
4. Provide the requested content on the Customer Information screen, then click Next to continue. The default values are appropriate for most installations.
5. Select one of the following installation types and then click Next to continue:
 - Typical: a typical installation is appropriate for most users.
 - Compact: a compact installation assumes that other features such as Enterprise Load Balancing are not required.
 - Custom: a custom installation allows you to modify more S-TAP installation options such as the software choices, installation directory, and the user account that runs the Windows S-TAP process.
6. Optional: Enable Enterprise Load Balancing by selecting the Enable Load Balancing checkbox on the Load Balancing Options screen. Click Next to continue.
 - a. If you enable Enterprise Load Balancing, provide the load balancer IP address in the Load Balancer Host Address field.
 - b. Click Advanced Options to specify any additional Enterprise Load Balancing options.
For more information, see [Enterprise Load Balancing](#).
7. Verify the Software Tap Host Address and provide Appliance Address(es) on the Network Addresses screen, then click Next to continue.
 - The Software Tap Host Address specifies the address of the database where the S-TAP is being installed.
 - One or more Appliance Addresses specify the Guardium system addresses that control the S-TAP. Provide multiple addresses (typically not more than three) on separate lines to establish failover systems for the S-TAP or when configuring S-TAP load balancing with the participate_in_load_balancing parameter.
Attention: If you do not want the S-TAP service to be enabled after installation, clear the Start S-Tap Service checkbox. If the S-TAP Service is not started, auto discovery of databases and creation of inspection engines is also disabled.
The Install Wizard Completed page appears after a successful installation.
8. Click Finish to close the installer.

What to do next

Verify that the S-TAP is communicating with the Guardium system by browsing to [Manage > Activity Monitoring > S-TAP Control](#) and reviewing the S-TAPs status and configuration.

Related tasks

- [Windows: Remove the S-TAP using Add/Remove Programs](#)
- [Windows: Uninstalling S-TAP using the command line](#)

Windows: Upgrading the S-TAP agent using the interactive installer

The interactive installer is useful for smaller deployments or whenever a guided, step-by-step installation experience is required.

Before you begin

Verify the following before you begin:

- Review the Windows S-TAP installation requirements at [Windows: Prerequisites: Installing S-TAP](#).
- Verify that your database server and operating system are supported. For more information, see [System requirements](#) and [Windows: S-TAP monitoring mechanisms support matrix](#).
- Identify the IP address of the database server where you will upgrade the S-TAP, including any virtual IP addresses.
- Obtain the S-TAP module from either [Fix Central](#), or your Guardium representative.

Note: You cannot install or run Windows S-TAP on a domain controller.

Note: **Db2 servers.** When upgrading an S-TAP from 11.3 or before to 11.4 or later on Db2 servers, the S-TAP cannot continue to capture the Db2 server traffic. Stop and restart your Db2 instances after the S-TAP upgrade to resume capturing Db2 traffic. Subsequent upgrades do not require you to restart the instances.

Procedure

1. Log on to the database server using a system administrator account.
2. Copy the S-TAP module to your database and start the Guardium Windows S-TAP Install Wizard.
Attention: When installing an S-TAP on Windows 2012 or later, you must use administrative privileges. To do this, right-click the installer and choose Run as Administrator.
3. Read the license agreement on the Guardium License screen. To continue installation, select I accept the terms of the license agreement and click Next.
4. Provide the requested content on the Customer Information screen, then click Next to continue. The default values are appropriate for most installations.
5. Select one of the following installation types and then click Next to continue:
 - Typical: a typical installation will be appropriate for most users.
 - Compact: a compact installation assumes that additional features such as Enterprise Load Balancing are not required.
 - Custom: a custom installation allows you to modify additional S-TAP installation options such as the software choices, installation directory, and the user account that runs the Windows S-TAP process.
6. Optionally enable Enterprise Load Balancing by selecting the Enable Load Balancing checkbox on the Load Balancing Options pane. Click Next to continue.
 - a. If you enable Enterprise Load Balancing, provide the load balancer IP address in the Load Balancer Host Address field.
 - b. Click the Advanced Options button to specify any additional Enterprise Load Balancing options.
For more information, see [Enterprise Load Balancing](#).
7. Verify the Software Tap Host Address and provide Appliance Address(es) on the Network Addresses screen, then click Next to continue.
 - The Software Tap Host Address specifies the address of the local machine where the S-TAP is being installed.
 - The Appliance Address(es) specify the Guardium® system addresses that will control the S-TAP. Provide multiple addresses (typically not more than three) on separate lines to establish failover systems for the S-TAP or when configuring S-TAP load balancing with the `participate_in_load_balancing` parameter.
Attention: If you do not want the S-TAP service to be enabled after installation, deselect the Start S-Tap Service checkbox. Deselecting the Start S-Tap Service checkbox also disables the automatic discovery of databases and creation of inspection engines.The Install Wizard Completed screen appears following a successful installation.
8. Click Finish to close the installer.

What to do next

Verify that the S-TAP is communicating with the Guardium system by navigating to [Manage](#) > [Activity Monitoring](#) > [S-TAP Control](#) and reviewing the S-TAPs status and configuration.

Windows: Use CLI to install, upgrade, uninstall the S-TAP

- [Windows: Installing S-TAP agent using the command line interface](#)
The command-line installer provides a scriptable solution that is especially useful for managing large deployments.
- [Windows: S-TAP command line installation parameters](#)
Understand the parameters (each with a short description) that you can use in your script and GIM installation.
- [Windows: Upgrading S-TAP using the command line](#)
You can upgrade the Windows S-TAP from the command line using the setup command.
- [Windows: Uninstalling S-TAP using the command line](#)
You can use the command line to uninstall S-TAP no matter how it was installed. (For GIM installs, best practice is to uninstall with GIM.)

Windows: Installing S-TAP agent using the command line interface

The command-line installer provides a scriptable solution that is especially useful for managing large deployments.

Before you begin

Verify the following before you begin:

- Review the Windows S-TAP installation requirements at [Windows: Prerequisites: Installing S-TAP](#).
- Verify that your database server and operating system are supported. For more information, see [System requirements](#) and the [Windows: S-TAP monitoring mechanisms support matrix](#).
- Identify the IP address of the database server where you are installing the S-TAP, including any virtual IP addresses.
- Identify the IP address of the Guardium® system that will control the S-TAP.
- Verify that the intended S-TAP installation directory is empty or does not exist.
- Obtain the S-TAP module from either [Fix Central](#), or from your Guardium representative.

Note: You cannot install or run Windows S-TAP on a domain controller.

Note: **Db2 servers.** When upgrading an S-TAP from 11.3 or before to 11.4 or later on Db2 servers, the S-TAP cannot continue to capture the Db2 server traffic. Stop and restart your Db2 instances after the S-TAP upgrade to resume capturing Db2 traffic. Subsequent upgrades do not require you to restart the instances.

About this task

If you want to disable auto-discovery, specify NOAUTODISCOVERY during the installation. For more information, see [Windows: Auto discovery of database instances during installation and upgrade](#).

Procedure

1. Log on to the database server using a system administrator account.
2. Copy the installer to your database, and using the Windows Command Prompt, navigate to the Windows S-TAP installer directory.
For example,

```
cd c:\Windows-STAP-V10.6.0.0.89
```

You should find a **setup.exe** executable in the installer directory.

3. Install the S-TAP using the **setup.exe** executable with the appropriate parameters.

The required parameters are:

- INSTALLPATH, the default is used if you do not specify
- TAPHOST
- APPLIANCE

All parameters, except INSTALLPATH, can be updated after the installation. A typical install command is:

```
setup.exe -UNATTENDED -APPLIANCE 10.0.147.234 -TAPHOST 10.0.145.41
```

where:

- -UNATTENDED (required) invokes the command-line installer.
- -APPLIANCE specifies the IP address of the Guardium system that will control the S-TAP.
- -TAPHOST (required) specifies the client IP address where the S-TAP is being installed.

For a complete description of the **setup.exe** executable and its parameters, see [Windows: S-TAP command line installation parameters](#).

What to do next

Verify that the S-TAP is communicating with the Guardium system by browsing to Manage > Activity Monitoring > S-TAP Control and reviewing the S-TAPs status and configuration.

Related reference

- [Windows: S-TAP command line installation parameters](#)

Windows: S-TAP command line installation parameters

Understand the parameters (each with a short description) that you can use in your script and GIM installation.

In a CLI installation, you install an S-TAP by using **setup.exe** with the appropriate parameters, as follows,

setup.exe -PARAMETER value

Do not use “=” signs to assign values to the parameters. The only time “=” is used when you want to add a parameter to the TAP section of the guard_tap.ini file directly as it is typed in the command line.

To add parameters that are not specified here but are required in the guard_tap.ini file, append the [TAP] section by specifying the parameter and value with an = sign, for example:

```
setup.exe -UNATTENDED -INSTALLPATH "C:\Program Files\IBM\Windows S-TAP" -APPLIANCE 10.0.148.160 -TAPHOST 10.0.146.160 QRW_INSTALLED=0  
QRW_DEFAULT_STATE=0
```

Important: The TAPHOST, APPLIANCE, INSTALLPATH attributes are required.

Attention: If a parameter is available through both the GIM and the command line interface (CLI), then the GIM parameter, including any defaults, always overwrites any value that is available from **WINSTAP_CMD_LINE**.

Table 1. Parameters applicable to all .NET installers

Command line parameter	GIM parameter	Description
UNATTENDED	QUIET	Install silently. (Does not require a value).
INSTALLPATH	WINSTAP_INSTALL_DIR	The installation directory. Default installation path is C:\Program Files\IBM\Windows S-TAP
UNINSTALL		Uninstall. A value is not required.
CUSTOMER		Change a customer name.
COMPANY		Change a company name.
SERVICEUSER		Specify a user to run the service under.
SERVICEPASSWORD		The password for the user.

Table 2. Other S-TAP Parameters

Command line parameter	Description
APPLIANCE	The SQLGUARD IP. You can set up multiple appliances by specifying this parameter multiple times, each with a unique value.
ENABLEGAM	Enables the Guardium Agent Monitor service (GAM).
DISCOVERY-PORT	S-TAP Discovery connects to the Guardium system with this port. Default=8443. Only used in UNATTENDED mode.

Command line parameter	Description
INSTALLERLOGPATH	Specifies the location for storing the S-TAP installer log files. Use this parameter if you don't want to use the default location (C:).
NOAUTODISCOVERY	Prevents database instance discovery from running during the installation. A value is not required. For more information, see Windows: Auto discovery of database instances during installation and upgrade .
START	Controls whether S-TAP is started or not after installation. Attention: This parameter defaults to on and can be disabled only by setting its value to 0. Any value other than 0 set the parameter to on.
TAPHOST	The local/client IP. Required for unattended installation.

Table 3. S-TAP Parameters that default to ON.. Unless otherwise noted, the default value for each parameter is ON. Enter any other value to turn off the parameter.

Command line parameter	GIM parameter	Description
V8PROTOCOL	WINSTAP_V8_PROTOCOL	Default = OFF. Note: To use V8 protocol, set this parameter to ON.
TCP	WINSTAP_TCP_DRIVE_R_INSTALLED	Use TCP driver.
NMP	WINSTAP_NAMED_PIPE_DRIVER_INSTALLED	Allows you to specify the named pipe used by MS SQL Server for local access. If a named pipe is used, but nothing is specified in this parameter, S-TAP attempts to retrieve the named pipe name from the registry. In rare cases, the S-TAP named pipes driver can interact with other third-party software in ways that slow the server down. To turn off the named pipes driver, set this parameter to 0. The named pipes driver is removed at the next system reboot. Note: If you turn off the named pipes driver, then the S-TAP does not capture named pipes traffic.
DB2SHMEM	WINSTAP_DB2_TAP_INSTALLED	Enables sniffing Db2 shared memory traffic.
DB2EXIT	WINSTAP_DB2_EXIT_DRIVER_INSTALLED	Enables Db2 integration with S-TAP.
ORACLEPLUGIN	WINSTAP_ORA_DRIVE_R_INSTALLED	Enables sniffing Oracle ASO and SSL traffic.

Table 4. Enterprise Load Balancing parameters

Command line parameter	GIM parameter	Description
LOAD-BALANCER-IP	WINSTAP_LOAD_BALANCER_IP	Required if you are configuring load balancing. This option specifies the IP address of the central manager or managed unit for the S-TAP to use for load balancing. <ul style="list-style-type: none"> • S-TAP parameters cannot be changed via the interactive installer during upgrade. Use the Guardium® UI after the upgrade to change S-TAP parameters. • To configure the enterprise load balancer to run on a managed unit, the S-TAP must be at V10.1 or higher.
LB-APP-GROUP	WINSTAP_INITIAL_BALANCER_TAP_GROUP	Optional. The application group name that this S-TAP belongs to for enterprise load balancing. Attention: Group names with spaces or special characters are not supported.
LB-MU-GROUP	WINSTAP_INITIAL_BALANCER_MU_GROUP	Optional. The managed unit group name to associate with the app-group. Requires a defined LB-APP-GROUP. A managed unit group must exist on the central manager before it can be used during installation of S-TAP. Attention: Group names with spaces or special characters are not supported.
LB-NUM-MUS	WINSTAP_LOAD_BALANCER_NUM_MUS	The number of managed units the enterprise load balancer allocates for this S-TAP.

Windows: Upgrading S-TAP using the command line

You can upgrade the Windows S-TAP from the command line using the setup command.

Before you begin

Note: **Db2 servers.** When upgrading the S-TAP V11.3 and lower to V11.4 and higher on DB2 servers, the S-TAP cannot continue to capture the DB2 server traffic. Stop and restart your Db2 instances after the S-TAP upgrade to resume capturing DB2 traffic. Subsequent upgrades do not require restart of the instances.

Procedure

1. Log on to the database server system using a system administrator account.
2. Change to the directory containing the S-TAP setup program.
3. Run the setup program with the following options: **setup -UNATTENDED**

Windows: Uninstalling S-TAP using the command line

You can use the command line to uninstall S-TAP no matter how it was installed. (For GIM installs, best practice is to uninstall with GIM.)

About this task

This procedure removes the installed S-TAP while making sure the configuration file is saved for future use. The Windows S-TAP can be uninstalled without reboot. Upgrade your S-TAP to 11.4 (or later), reboot the S-TAP once, for example, in the next maintenance window. Then, you can uninstall the S-TAP without rebooting the database server or restarting database instances. A fresh install of the 11.4 (or later) S-TAP out of the box is fully uninstallable without requiring a reboot.

Procedure

1. Log on to the database server system using a system administrator account.
2. Copy the current S-TAP configuration file to a safe location (a non-Guardium directory). Look for this file in C:\Program Files (x86)\IBM\Windows S-TAP\Bin\guard_tap.ini.
3. Change to the directory containing the S-TAP setup program.
4. Run the setup program with the following options: **setup -UNINSTALL**

Windows: Remove the S-TAP using Add/Remove Programs

You can use Add/Remove Programs to uninstall S-TAP no matter how it was installed. (For GIM installs, best practice is to uninstall with GIM.)

About this task

This procedure removes the installed S-TAP while making sure the configuration file is saved for future use.

Procedure

1. Log on to the database server system using a system administrator account.
2. Copy the current S-TAP configuration file to a safe location (a non-Guardium directory). Look for this file in C:\Program Files\IBM\Windows S-TAP\Bin\guard_tap.ini.
3. From the Add/Remove Programs control panel, remove IBM® Security Guardium® S-TAP.

Windows: S-TAP installation flow on Oracle RAC

Configure S-TAPs in an Oracle RAC.

Procedure

1. Install S-TAP on all nodes. In case GIM is used, install GIM client on all nodes, then install S-TAP on all nodes.
2. Configure the S-TAP parameter STAP_TAP_IP: public IP configured for the node. (Can be configured through GIM UI.)
 - The parameter STAP_ALTERNATE_IPS is not required.
 - If the Oracle database is encrypted (ASO/SSL) make sure the parameter ORA_DRIVER_INSTALLED=1
 - If the Oracle inspection engine is auto-discovered, it already contains all required parameters including INSTANCE_NAME.

Windows: Managing S-TAP when upgrading your database

Use these guidelines for managing your Windows S-TAP when upgrading your database.

Procedure

1. Upgrade your database.
2. If using exit: make sure the exit library is in the appropriate place (for example if there is a new DB location directory).
3. Check that the inspection engine for the database is correct (for example, the version number).
4. If changes in the IE were made, restart the S-TAP.

Windows: Managing S-TAP when upgrading your database operating system

Use these guidelines for managing an S-TAP, when upgrading the operating system (OS) of your database. This is relevant for all S-TAPs, regardless of the installation method.

Before you begin

- Verify that the installed Windows S-TAP agent supports the new OS version. If not, upgrade Windows S-TAP before or after upgrading the OS, using the same method as the S-TAP installation. See the [Guardium support matrix](#).

About this task

The GIM parameter auto_install_on_db_server_os_upgrade controls GIM's ability to auto-upgrade all bundles. If enabled, when the database server boots up after an operating system upgrade, GIM automatically downloads and installs these bundles. This parameter is disabled by default to prevent unintentional bundle upgrades. It's easiest to enable the parameter before you upgrade the database operating system.

If the parameter is disabled when you upgrade the database operating system, the GIM client detects that the operating system changed, and it changes the _x suffix of the version to _0. You can see the version in the Set up by Client, for example, 10.6.1.4_r123456_0. To resolve the mismatch between the GIM client and the database operating system, do one of:

- Enable the GIM global parameter auto_install_on_db_server_os_upgrade, which automatically upgrades all the GIM clients with the latest bundle of the operating system they support.
- Do not enable auto_install_on_db_server_os_upgrade, and upgrade the GIM clients manually.

It is best to update all your GIM-installed modules as soon as possible after the upgrade, whether manually or automatically. K-TAP is not loaded after an operating system upgrade.

Procedure

1. Back up the guard_tap.ini file. You probably won't need it, but retain it until the S-TAP is functioning as expected after the upgrade.
2. Upgrade the operating system of the database.
3. Restart Windows S-TAP.

Related tasks

- [Windows: Starting S-TAP using GIM](#)
- [Windows: Starting S-TAP without GIM](#)
- [Windows: Upgrading S-TAP agent with GIM Setup by Client](#)
- [Windows: Upgrading the S-TAP agent using the interactive installer](#)
- [Windows: Upgrading S-TAP using the command line](#)

Windows: When to restart or reboot the database server after installing or upgrading S-TAP

In general, you do not need to reboot the database server after you install or upgrade Windows S-TAP unless you are upgrading between versions or when stated otherwise in the release notes.

You do not need to reboot for any fresh S-TAP installation.

However, you do need to reboot the database server to update the NmpProxy driver when you upgrade between versions. For example, a reboot is required if you upgrade from Windows S-TAP 11.2 (or earlier) to 11.3 (or later). However, if there are no issues with your current NmpProxy functionality, you can delay the reboot until the next maintenance cycle.

If you are not certain about reboot requirement for particular version you are using, check with your Technical Support representative. Restart/reboot requirements are the same for GIM and non-GIM implementations.

Reboot database servers only when you need to upgrade the driver.

Windows: Managing S-TAP when upgrading your database

Use these guidelines for managing your Windows S-TAP when upgrading your database.

Procedure

1. Upgrade your database.
2. If using exit: make sure the exit library is in the appropriate place (for example if there is a new DB location directory).
3. Check that the inspection engine for the database is correct (for example, the version number).
4. If changes in the IE were made, restart the S-TAP.

Windows: Managing S-TAP when upgrading your database operating system

Use these guidelines for managing an S-TAP, when upgrading the operating system (OS) of your database. This is relevant for all S-TAPs, regardless of the installation method.

Before you begin

- Verify that the installed Windows S-TAP agent supports the new OS version. If not, upgrade Windows S-TAP before or after upgrading the OS, using the same method as the S-TAP installation. See the [Guardium support matrix](#).

About this task

The GIM parameter auto_install_on_db_server_os_upgrade controls GIM's ability to auto-upgrade all bundles. If enabled, when the database server boots up after an operating system upgrade, GIM automatically downloads and installs these bundles. This parameter is disabled by default to prevent unintentional bundle upgrades. It's easiest to enable the parameter before you upgrade the database operating system.

If the parameter is disabled when you upgrade the database operating system, the GIM client detects that the operating system changed, and it changes the _x suffix of the version to _0. You can see the version in the Set up by Client, for example, 10.6.1.4_r123456_0. To resolve the mismatch between the GIM client and the database operating system, do one of:

- Enable the GIM global parameter auto_install_on_db_server_os_upgrade, which automatically upgrades all the GIM clients with the latest bundle of the operating system they support.
- Do not enable auto_install_on_db_server_os_upgrade, and upgrade the GIM clients manually.

It is best to update all your GIM-installed modules as soon as possible after the upgrade, whether manually or automatically. K-TAP is not loaded after an operating system upgrade.

Procedure

1. Back up the guard_tap.ini file. You probably won't need it, but retain it until the S-TAP is functioning as expected after the upgrade.
2. Upgrade the operating system of the database.
3. Restart Windows S-TAP.

Related tasks

- [Windows: Starting S-TAP using GIM](#)
 - [Windows: Starting S-TAP without GIM](#)
 - [Windows: Upgrading S-TAP agent with GIM Setup by Client](#)
 - [Windows: Upgrading the S-TAP agent using the interactive installer](#)
 - [Windows: Upgrading S-TAP using the command line](#)
-

Windows: Configuring S-TAP

Learn to configure the S-TAP.

- [Windows: Configuring S-TAP in the S-TAP Control page](#)
Use the S-TAP Control page to view all S-TAPs that are managed by this Guardium system, manage individual S-TAPs, and perform a few operations on all S-TAPs.
 - [Windows: Configuring S-TAP with guard_config_update](#)
You can use the guard_config_update script to update your S-TAP configuration (without using the GUI).
 - [Windows: Discover database instances](#)
The instance discovery agent runs once per day, by default. It reports new database instances, listener, and port information to the Guardium® system. It does not update the inspection engine configurations.
 - [Windows: Configuring an Inspection Engine](#)
Configure or modify an inspection engine in the S-TAP Control pane.
 - [Windows: Inspection engine verification](#)
S-TAP verification confirms that the S-TAPs and their inspection engines in your environment are running and actively monitoring database activity. Understand verification, and define a schedule to regularly verify S-TAPs.
 - [Windows: S-TAP load balancing models and configuration guidelines](#)
Understand the S-TAP load balancing models, and choose the one appropriate to your setup.
 - [Windows: Configuring the Db2 Exit library](#)
The Db2 Exit mechanism enables Guardium to pick up all Db2 traffic, whether encrypted or not and whether local or remote. This solution simplifies the S-TAP configuration, and provides native Db2 support.
 - [Windows: Upload dump files from the S-TAP to the collector and central manager](#)
You can configure the S-TAP to automatically upload dump files upon restart, to the collector and the central manager, or only the collector.
 - [Windows: Build and configure FreeTDS for Guardium](#)
FreeTDS allows Unix/Linux machines to connect to an SQL Server on Windows machines.
-

Configuring S-TAP in the S-TAP Control page

Use the S-TAP Control page to view all S-TAPs that are managed by this Guardium system, manage individual S-TAPs, and perform a few operations on all S-TAPs.

Before you begin

You must be logged in to a Guardium system that is the active host for the S-TAP.

About this task

During the installation process, a user might make an error in configuring an S-TAP, which is not detected until after the installation process finishes. For instance, a user might forget to enter an IP address or use the wrong IP address when they define an SQL Guard IP. To remedy these types of mistakes, you can modify some of the S-TAP configurations.

You can safely change the parameters that are in the GUI. Parameters that do not appear in the GUI are advanced parameters. Do not change them without instructions from Guardium support.

All configuration changes require that you restart the S-TAP agent. If you modify parameters in the GUI or with GIM, the S-TAP is restarted transparently. If you need to restart the S-TAP manually (for example after you modify the configuration by using API or directly in the guard_tap.ini file), use the [Send command](#), or see [Windows: Starting S-TAP using GIM](#), or [Windows: Starting S-TAP without GIM](#).

If you installed your S-TAP by using the Guardium Installation Manager (GIM), you can update some parameters through the GIM GUI or API.

S-TAP status can be one of:

- Green: Online
 - Yellow: Indicates an S-TAP or a database server error. To see details about a specific error, click  to open the S-TAP event log.
Typical errors, along with their resolutions, include:
 - CPU exceeds threshold: The CPU_USAGE_LIMIT is exceeded by the number of minutes determined by CPU_USAGE_INTERVALS_ALLOWED.
Resolution: Take one of the following steps:
 - Restart the S-TAP.
 - Increase the system CPU.
 - Verify and, if needed, modify, the CPU parameter values in either the guard_tap.ini file or through the GIM parameters.
 - Handle count exceeds threshold: The HANDLE_COUNT_LIMIT is exceeded by the number of minutes determined by HANDLE_COUNT__INTERVALS_ALLOWED.
Resolution: Take one of the following steps:
 - Restart the S-TAP.
 - Verify and, if needed, modify, the HANDLE_COUNT parameter values in either the guard_tap.ini file or through the GIM parameters.
 - S-TAP memory usage exceeds threshold: The MEM_USAGE_LIMIT is exceeded by the number of minutes determined by MEM_USAGE_INTERVALS_ALLOWED.
Resolution: Take one of the following steps:
 - Restart the S-TAP.
 - Increase S-TAP memory.
 - Verify and, if needed, modify, the S-TAP memory values in either the guard_tap.ini file or through the GIM parameters.
 - DBMonitor service down.
Resolution: Restart the S-TAP by clicking Accept.
 - DLLs not loaded correctly: Certain DLLs that support Db2 Exit or encrypted traffic might not be loaded correctly.
Resolution: Verify the relevant parameters in guard_tap.ini and then restart the S-TAP.
 - Drivers not running or loaded: An issue exists with the S-TAP drivers.
Resolution: Restart the drivers manually by running the net start <driver_name> command from an administrative command prompt. The driver name is included in the error message.
- The S-TAP drivers for your system depend on the S-TAP protocol. For more information about protocols, see [Windows: S-TAP protocol 8](#). For more information about the S-TAP drivers, see either, [Driver parameters](#) or [Protocol 8 Driver parameters](#).
- Load Balancer is down: The load balancer is unreachable by the S-TAP.
Resolution: Check the load balancer and restart if needed. Verify the load balancer IP address by clicking Modify. If you make changes, click Accept.
 - Out of range ini parameter values: One or more S-TAP parameters in the TAP section of the guard_tap.ini file are outside of the acceptable range.
Resolution: Modify the relevant parameter values by taking one of the following steps:
 - Click Modify, if available (not all parameters can be modified from the Modify page) and then click Accept
 - Modify the parameters from the guard_tap.ini file.
 - Modify the parameters from GIM.

If problems persist, contact Guardium support.

Note: When you modify S-TAP parameters in the GUI or through the GuardAPI, S-TAP checks the values before it saves the parameters. When the S-TAP identifies an erroneous value, the value is not saved and Guardium creates an error in the S-TAP event log. The S-TAP uses default values so that it can keep sending traffic.

- Red: Offline

Procedure

1. Click Manage > Activity Monitoring > S-TAP Control to open S-TAP Control.

2. Perform operations on all S-TAPs in the page.

- Refresh: Refresh display of S-TAPs.
- Add All to Schedule: Add all displayed S-TAPs to the S-TAP verification schedule. See [Windows: Inspection engine verification](#).
- Remove All from Schedule: Remove all displayed S-TAPs from the S-TAP verification schedule.
- Comments: Add comments. See [Comments](#).

3. Identify the S-TAP to be configured by its IP address or the symbolic hostname of the database server on which it is installed. View and perform operations on individual S-TAPs.

Option	Description
Delete: 	Click Delete to remove an S-TAP. Deleting S-TAPs is useful to clean up your display when you know that an S-TAP is inactive, or when the Guardium unit is no longer listed as a host in the S-TAP's configuration file. In either of these cases, the S-TAP displays indefinitely with an offline status if you do not delete it. You cannot remove an active S-TAP from the list. Clicking Delete does not stop an S-TAP from sending information, and does not remove the Guardium host from the list of hosts that are stored in the S-TAP's configuration file.
Refresh: 	Click Refresh to fetch a copy of the latest S-TAP configuration from the agent. The S-TAP display does not auto-refresh.

Option	Description
Send Command: 	Opens the S-TAP Commands window, where you can run various commands on the S-TAP host. <ul style="list-style-type: none"> • Restart. Restarts the S-TAP in the mode you select. <ul style="list-style-type: none"> • 0: Restarts the S-TAP. Use this mode in environments without enterprise load balancing. • 1: Restarts the S-TAP process while preserving the data in the S-TAP buffer. (The S-TAP picks up the new configuration from the enterprise load balancer without flushing the buffers.) Used in the enterprise load balancer environment. • S-TAP logging: Starts S-TAP logging for debugging purposes, at the log level you enter in Level and for the duration you enter in Duration Sec. See DEBUGLEVEL in Debug parameters and Protocol 8 Debug parameters. • Run Diagnostics: Run the S-TAP diagnostics script (and upload the results to the Guardium system) • Revoke Ignore: All sessions that are ignored by a revocable ignore policy become available, and S-TAP starts capturing the traffic for those sessions. • Run Database Instance Discovery: Runs the database instance discovery once, immediately. (By default, it runs once every 24 hours.) Select Replace Inspection Engines only if you want to override defined inspection engines with discovered details, and restart the S-TAP. For a full description of this option, see Windows: Discover database instances. You can specify rules that manage how discovered details on database instances are implemented, or not. For more information, see Database discovered instances rules.
Edit S-TAP configuration: 	Opens the S-TAP configuration window. Parameters that do not appear in the GUI are advanced parameters. Do not modify them unless you are an advanced user, or you are instructed to modify them by Guardium Technical Support. <ul style="list-style-type: none"> • S-TAP Control: Details • S-TAP Control: Change auditing • S-TAP Control: Application server user identification • S-TAP Control: Guardium Hosts • S-TAP Control: Firewall Details • S-TAP Control: Inspection Engines
Show S-TAP Event Log: 	Click to open the S-TAP event log, where you can see events such as connect, disconnect, GIM server configuration. This log is useful for troubleshooting.
Add to Schedule	If selected, adds the individual S-TAP to the scheduled verification.
Revoke All Ignored Sessions	A database might be running many sessions, some of which are currently ignored. Clear this option to stop ignoring traffic from ignored sessions.

- [S-TAP Control: Details](#)
Understand the parameters in the Details section of the S-TAP Control in the GUI.
- [S-TAP Control: Change auditing](#)
Understand the parameters in the Change Auditing section of the S-TAP Control in the GUI.
- [S-TAP Control: Application server user identification](#)
Understand the parameters in the Application server section of the S-TAP Control in the GUI.
- [S-TAP Control: Guardium Hosts](#)
Understand the parameters in the Guardium Hosts section of the S-TAP Control in the GUI.
- [S-TAP Control: Firewall Details](#)
These parameters affect the behavior of the S-TAP with respect to the firewall.
- [S-TAP Control: Inspection Engines](#)
Understand the parameters in the Inspection Engines section of the S-TAP Control page.

S-TAP Control: Details

Understand the parameters in the Details section of the S-TAP Control in the GUI.

Parameter	Default value	Description
Version		The S-TAP version.
Devices	none	Which interfaces to listen on. Use ifconfig to find the correct interface.
Load balancing	0	<p>Controls S-TAP load balancing to Guardium® systems. Valid values:</p> <ul style="list-style-type: none"> • 0: No load balancing. • 1: Load balancing. Traffic is balanced between the primary and secondary servers, which are defined in the SQLGuard section. • 2: Redundancy. Fully mirrored S-TAP sends all traffic to all primary and secondary servers, which are defined in the SQLGuard section. • 3: Hardware load balancing. Guardium uses a load balancer such as F5 or Cisco. S-TAP sends the traffic to the load balancer, which forwards it to one of the collectors in the pool. <p>Use the primary parameter in the Guardium Hosts section to specify primary, secondary, tertiary, or more, servers. If this parameter is set to 0, and you have more than one Guardium system monitoring traffic, then the non-primary Guardium systems are available for failover.</p> <p>This parameter is also used in enterprise load balancing. For more information, see Enabling enterprise load balancing and associating an S-TAP with a central manager.</p>
Trace files dir	INSTALLDIR	The Directory in which access tracer files are stored.
App. server user Identification		

Parameter	Default value	Description
TLS Use	0	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> do not encrypt traffic between the S-TAP agent and the Guardium system. Warning: The traffic between the agent and Guardium system is in clear text. <input checked="" type="checkbox"/> Use SSL to encrypt traffic between the S-TAP agent and the Guardium system. <p>Guardium recommends encrypting network traffic between the S-TAP and the collector whenever possible. Only in cases where the performance is a higher priority than security should this be disabled.</p>
Compress. level	0	Data compression level, from 1 to 9. 0=no compression.
All can control	0	Defines which Guardium system control this S-TAP. Valid values: <ul style="list-style-type: none"> <input checked="" type="checkbox"/> S-TAP is controlled by the primary Guardium system only. <input checked="" type="checkbox"/> S-TAP can be controlled by any Guardium system.
Load Balancer host name or IP address		<p>The IP address of the central manager or managed unit this S-TAP should use for load balancing.</p> <ul style="list-style-type: none"> If using enterprise load balancing while Load balancing and Managed units, failover data is not sent to the secondary system. Instead, failover data is sent to the system allocated by the load balancer to replace the failed server. This is true only as long as the Central Manager is running and Enterprise Load Balancer is active. If the load balancer is not available then traffic is rerouted to secondary sqlguard_ip. S-TAP parameters cannot be changed via the interactive installer during upgrade. Use the Guardium UI after the upgrade to change S-TAP parameters. If configuring the enterprise load balancer to run on a managed unit, the S-TAP must be at V10.1 or higher.
Managed Units		The number of managed units the enterprise load balancer allocates for this S-TAP.
Restricted logging		Controls restricted logging on the collector. Use this to evaluate the number of records affected by an SQL command, while masking the actual query. This parameter can only be set by user root on the DB server. Valid values: <ul style="list-style-type: none"> 0: Unrestricted. 1: Log with masking. Only logins are allowed (sent packets are flagged with LOGALWAYSMASK). Forces encryption to be on in the S-TAP regardless of any other settings; traffic is sent to the collector only after the collector has indicated that it is aware of the parameter value. Otherwise, the S-TAP logs a message that traffic can't be sent, and its status is red in the S-TAP Control page. 2: All packets are allowed (sent packets are flagged with LOGACCESSIONLY)
Discovery interval		<p>The interval at which the S-TAP reports database instance discovery results to the collector. Select only if you want to change the discovery interval from its default of 24 hours. When you select this option, the UI updates with two radio buttons: Hour and Minute. Type in any positive integer to set the discovery interval in either hours or minutes. Valid values:</p> <ul style="list-style-type: none"> Hours: maximum of 24 Minutes: 5 - 1440 <p>Clear the Enable discovery interval checkbox to disable.</p>

S-TAP Control: Change auditing

Understand the parameters in the Change Auditing section of the S-TAP Control in the GUI.

GUI	Default value	Description
Task checkpoint	task_checkpoint	Internal handle program machine state in case of host failure.
Client checkpoint	client_checkpoint	File used to restart processing. A series of files is created. Each version of the file ends with a unique number.
Checkpoint period	3600	Interval time, in seconds, for the check.
Fail over file	fail_over_file	Name of the outgoing messages buffer. The database writes to this file when the Guardium® system cannot be reached. During this time, the file can grow to the maximum size specified. When the limit is reached, a second file is created, with the same name with the digit 2 appended to the end of the name. (At this point CAS begins trying to connect to a secondary server.) If that file also reaches the maximum size, the first file is overwritten. If the first file fills again, the second file is overwritten. Thus, following an extended outage, you might lose data, but an amount of data up to twice the size of the Failover File Size Limit is stored.
Fail over file size limit	50000	Failover file maximum size, in KB. The disk space requirement is twice what you specify here because the system maintains two failover files. If you specify -1, the file size is unlimited, but it is recommended that you cap the file size.
Max rec. attempts	5000	Number of reconnect attempts when connection is lost. The maximum number of times CAS attempts to reconnect to the Guardium system. Set this value to -1 for unlimited reconnection attempts. The default cas_max_reconnect_attempts and cas_reconnect_interval define an interval of about 3.5 days. After reaching the maximum, CAS continues to run, writing to the failover files, but it does not attempt to reconnect with a Guardium host.
Reconnect interval	60	Wait time, in seconds, between reconnect attempts.
Raw data limit	1000	Maximum number of KB written for an item when the Keep data checkbox is marked in the item template. If you specify -1, the size is unlimited.
Md5 size limit	1000	Maximum size of a data item, KB, on which the MD5 checksum calculation is performed. If you specify -1, there is no limit.

S-TAP Control: Application server user identification

Understand the parameters in the Application server section of the S-TAP Control in the GUI.

Parameter	Default value	Description
Session timeout		
Ports	8080	Comma-separated list of ports, or hyphens for inclusive ranges of ports, on which the Java™ application is accessed by a web browser.
Login pattern		Comma-separated list of strings specifying the login pattern that is passed to the application. This pattern is passed to the Java application to identify a user login.
Username prefix		Comma-separated list of strings specifying the prefix to the username for a given session. This is the pattern the Java application uses to indicate the username of the given session.
Username postfix		Comma-separated list of strings specifying the postfix to the username for a specific session. This pattern is passed to the Java application to indicate the end of the value for the given variable that indicates the username.
Session pattern		Comma-separated list of strings specifying the start of an end-user session, using a particular database session. This pattern specifies the [change of] end-user session for a specific database connection.
Session prefix		Comma-separated list of strings specifying the session identifier.
Session postfix		Comma-separated list of strings specifying where the session ends.
Session ID pattern		Comma-separated list of strings specifying the identifier for marking which end-user session a specific connection is continuing with.
Session ID prefix		Comma-separated list of strings specifying what identifies or precedes the session_id in a specific users indicator packet.
Session ID postfix		Comma-separated list of strings specifying where the session ID ends.

S-TAP Control: Guardium Hosts

Understand the parameters in the Guardium Hosts section of the S-TAP Control in the GUI.

Parameter	Description
Guardium Host	IP address or hostname of the Guardium system that acts as the host for the S-TAP. You can define multiple hosts by clicking Modify, and opening the Guardium Hosts section.
Active	<ul style="list-style-type: none"> • <input checked="" type="checkbox"/> : connection is active. • <input type="checkbox"/> : connection is not active. <p>You can change the primary S-TAP by clicking Modify, and opening the Guardium Hosts section.</p>

S-TAP Control: Firewall Details

These parameters affect the behavior of the S-TAP with respect to the firewall.

Name	Default value	Description
Firewall installed		Firewall feature enabled. Valid values: <ul style="list-style-type: none"> • <input checked="" type="checkbox"/> : disabled. • <input type="checkbox"/> : enabled.
Firewall timeout	10	Time, in seconds, to wait for a verdict from the Guardium® system. If the firewall times out, the value of the parameter Firewall fail close determines whether to block or allow the connection. Valid values: 0-10.
Firewall default state	0	Valid values: <ul style="list-style-type: none"> • 0: Firewall is activated per session when triggered by a rule in the installed policy. • 1: All traffic is watched for firewall policy violations • 2: All traffic is watched for firewall policy violations for the initial priority_count packets (guard_tap.ini parameter). S-TAP watches the initial part of every new session to your DB. This is useful when you have session based policies, firewall rules based on the user, or some other information that is passed early in the session. It limits the impact of firewall on the performance. Instead of watching every bit of the session (Firewall default state=1) and waiting for an UNWATCH verdict, S-TAP simply unwatches automatically if no WATCH or DROP is sent.
Firewall fail close	<input checked="" type="checkbox"/>	The action when the verdict cannot be set by the policy rules, for example the Firewall timeout expires. Valid values: <ul style="list-style-type: none"> • <input checked="" type="checkbox"/> : the connection goes through. • <input type="checkbox"/> : the connection is blocked.
Firewall force watch		When Firewall default state=0 (off), then Firewall force watch specifies the network/mask of the IPs you want the firewall to watch, overriding the default (off). Valid value: comma separated list of IP/mask values.
Firewall force unwatch		When Firewall default state=1 (on), then Firewall force unwatch specifies the network/mask of the IPs you want the firewall to ignore, overriding the default (on). Valid value: comma separated list of IP/mask values.

S-TAP Control: Inspection Engines

Understand the parameters in the Inspection Engines section of the S-TAP Control page.

Each inspection engine has a set of parameters. The parameters for each IE depend on the type of database.

Note: Inspection engines are created automatically. Do not change the parameter values unless instructed to do so by Technical Support.

Parameter	Default value	Description
Protocol		The type of data repository being monitored.
Instance Name		The name of the database instance on this server. Required when MS SQL Server is using encryption, or MS SQL Server using Kerberos Authentication. (MSSQLSERVER is the default.)
Port range		Starting port range specific to the database instance. Together with port_range_end defines the range of ports monitored for this database instance. There is usually only a single port in the range. For a Kerberos inspection engine, set the start and end values to 88-88. If a range is used, do not include extra ports in the range, as this could result in excessive resource consumption while the S-TAP attempts to analyze unwanted traffic.
Port range		Ending port range specific to the database instance.
Named Pipe		Specifies the named pipe used by MS SQL Server for local access. If a named pipe is used, but nothing is specified in this parameter, S-TAP attempts to retrieve the named pipe name from the registry.
KTAP DB Real Port	4100	Used only when the K-TAP monitoring mechanism is used. Identifies the database port to be monitored by the K-TAP mechanism.
Client Ip/Mask		<p>Identifies the clients to be monitored, using a list of addresses in IP address/mask format: n.n.n/n.m.m.m. If an improper IP address/mask is entered, the S-TAP does not start. Valid values:</p> <ul style="list-style-type: none"> • null=select all clients • 127.0.0.1/255.255.255.255=local traffic only <p>networks and exclude networks cannot be specified simultaneously. If the IP address is the same as the IP address for the database server, and a mask of 255.255.255.255 is used, only local traffic will be monitored. An address/mask value of 1.1.1.1/0.0.0.0 monitors all clients.</p>
Exclude Client Ip/Mask		A list of client IP addresses and corresponding masks that are excluded from monitoring. This option allows you to configure the S-TAP to monitor all clients, except for a certain client or subnet (or a collection of these). networks and exclude networks cannot be specified simultaneously.
TEE Listen Port-Real Port	12344	Deprecated. Replaced by the parameter real_db_port when the K-TAP monitoring mechanism is used. Was required when the TEE monitoring mechanism. The Listen Port is the port on which S-TAP listens for and accepts local database traffic. The Real Port is the port to which S-TAP forwards traffic.
Connect To Ip	127.0.0.1	IP address for S-TAP to use to connect to the database. Some databases accept local connection only on the real IP address of the machine, and not on the default (127.0.0.1). When K-TAP is enabled, this parameter is used for Solaris zones and AIX WPARs and it should be the zone IP address in order to capture traffic. When Tee is enabled, this parameter is the IP address for S-TAP to use to connect to the database. Some databases accept local connection on 127.0.0.1, while others accept local connection only on the 'real' IP of the machine and not on the default (127.0.0.1).
DB User		
DB Install Dir	NULL	DB2, Informix, or Oracle: Enter the full path name for the database installation directory. For example: /home/oracle10. All other database types enter: NULL
Process Name		Database's running executables that are to be monitored. For example, a DB2 IE would be TAP_DB_PROCESS_NAMES=DB2SYSCS.EXE
DB2 Shared Mem. Adjust.	20	Required when DB2 is selected as the database type, and shared memory connections are monitored. The offset to the server's portion of the shared memory area. Offset to the beginning of the DB2 shared memory packet, depends on DB2 version, 32 in the earlier versions, 80 in 8.2.1 and later.
DB2 Sh. Mem. Client Pos.	61440	The offset to the client's portion of the shared memory area. Required when DB2 is selected as the database type, and shared memory connections are monitored. The client offset can be calculated by taking the value of the DB2 parameter ASLHEAPSZ and multiplying by 4096 to get the appropriate offset. The default for this parameter is 61440 decimal. This parameter is calculated by taking the DB2 database configuration value of ASLHEAPSZ and multiplying by 4096. To get the value for ASLHEAPSZ, execute the following DB2 command: db2 get dbm cfg and look for the value of ASLHEAPSZ. This value is typically 15 which yields the 61440 default. If it's not 15, take the value and multiply by 4096 to get the appropriate client offset.
DB2 Shared Mem. Size		DB2 shared memory segment size. Required when DB2 is selected as the database type, and shared memory connections are monitored.
	NULL	For Oracle or MS SQL Server only, when named pipes are used. For Oracle, the list usually has two entries: oracle.exe,tnslsnr.exe. For MS SQL Server, the list is usually just one entry: sqlservr.exe. For a DB2, Oracle, or Informix database, enter the full path name for the database executable. For example: <ul style="list-style-type: none"> • Oracle: /home/oracle10/prod/10.2.0/db_1/bin/oracle • Informix: /INFORMIXTMP/.inf.sqlexec. Applies to all Informix platforms but Linux. • Informix with Linux, example: /home/informix11/bin/oninit • MYSQL: mysql • All other database types: NULL
Encryption	0	Activate ASO or SSL encrypted traffic for Oracle (versions 11 and 12) and Sybase on Solaris, HPUX and AIX. For Oracle, specify db_version in the ini file (e.g. db_version=12) For any Oracle requiring instrumentation, if you are using encryption=1 in the guard_tap.ini (which is not supported on Linux), you must instrument prior to setting that parameter.
	1	1=database traffic participates in load balancing. 0=database traffic does not participate in load balancing.
Intercept Types	NULL	Protocol types that are intercepted by the IE. Valid values: <ul style="list-style-type: none"> • NULL: auto intercepts all protocols the Database supports • Comma separated list: IE intercepts these protocol types only.
Identifier	NULL	Optional. Used to distinguish inspection engines from one another. If you do not provide a value for this field, Guardium auto populates the field with a unique name using the database type and GUI display sequence number.

Parameter	Default value	Description
DB Version	9	The database version. Used for capturing A-TAP traffic.
Unix Socket Marker	Null	Specifies UNIX domain sockets marker for Oracle, MySQL and Postgres. Usually the default value is correct, but when the named pipe or UNIX domain socket traffic does not work then you need to make sure this value is set correctly. For example, for Oracle, unix_domain_socket_marker should be set to the KEY of IPC defined in tnsnames.ora. If it is NULL or not set, the S-TAP uses defined default markers identified as: * MySQL - "mysql.sock" * Oracle - "./oracle/" * Postgres - ".s.PGSQL.5432"

Windows: Configuring S-TAP with `guard_config_update`

You can use the `guard_config_update` script to update your S-TAP configuration (without using the GUI).

About this task

Note: Parameter names are not case-sensitive.

Procedure

- From an administrative command prompt, browse to Windows S-TAP_>Bin.
- Run `guard_config_update` with the parameters that you need to set for your environment.

Parameter	Description
--help (or -h)	List all of the <code>guard_config_update</code> parameters.
--list-ie	List the names of all inspection engines, such as Db2 or MSSQL, on this machine.
--list-sqlguard	List the SQLGUARD address for this machine. For example: <code>VM02.TEST.MYCOMPANY.COM</code>
--list-all-tap-parameters	List the parameters that are in the Tap section. For information about individual parameters, see either Editing the protocol 7 and protocol 8 S-TAP configuration parameters or Editing the protocol 8 S-TAP configuration parameters depending on which protocol your site uses. Note: The output includes some hidden parameters.
--list-sections sectionName	List the section name and associated values in the specified <code>sectionName</code> , for example: <code>guard_config_update.exe --list-sections sqlguard [SQLGUARD_VM02.TEST.MYCOMPANY.COM] PRIMARY=1 SQLGUARD_IP=vm02.test.mycompany.com</code>
--list-services	Lists all S-TAP related services and their associated statuses.
--set-tap-parameter parmName1=parmValue1;parmName2=parmValue2...	Change one or more Tap parameters, where: <ul style="list-style-type: none">• parmName = The name of the parameter to change.• parmValue = The new value for the parameter. For example: <code>guard_config_update.exe --set-tap-parameter upload_feature=1;TENANT_ID=stuff10;ALL_CAN_CONTROL=1 Updated Tap section upload_feature=1 Updated Tap section TENANT_ID=stuff10 Updated Tap section ALL_CAN_CONTROL=1</code>
--set-tap-parameter-force parmName1=parmValue1;parmName2=parmValue2...	Change the specified parameter values for parameters that you cannot change in GIM.
--set-service serviceName1=action1;serviceName2=action2...	Configure one or more S-TAP related services on the database server to perform a specified action, where <code>action</code> can be one of the following: <ul style="list-style-type: none">• Service status:<ul style="list-style-type: none">• start• stop• restart• Windows settings Startup type:<ul style="list-style-type: none">• enable - Set to <i>Automatic</i>.• disable - Set to <i>Disabled</i>.
--set-sqlguard-ip ip/hostname	Change the address or hostname of the primary SQLGUARD appliance. Note: You can change only the primary SQLGUARD IP address.
--set-sqlguard section1,parmName1=parmValue1;section2,parmName2=parmValue2...	Modify the values for one or more SQLGUARD sections.
--set-ie section1,key1=value1;key2=value2...	Modify inspection engine values.
--add-sqlguard sectionName1;sectionName2..	Add an appliance (SQLGUARD) to the guard-tap.ini.

Parameter	Description
--add-ie sectionName1,key1=value1;key2=value2	Modify inspection engines values. To see the value in an inspection engine, use the --list-sections parameter. For example: C:\Program Files\IBM\Windows S-TAP\Bin>guard_config_update.exe --list-ie COUCH1 COUCHBASE1 DB21 ... C:\Program Files\IBM\Windows S-TAP\Bin>guard_config_update.exe --list-sections DB21 [DB_DB21] DB2_CLIENT_OFFSET=61440 DB2_FIX_PACK_ADJUSTMENT=80 DB_TYPE=DB2 DB_VERSION=11 ...
--remove-ie sectionName1,sectionName2	Remove inspection engines by section name.
--remove-sqlguard sectionName1,sectionName2..	Remove sections by the SQLGUARD section name.

3. When you are done, restart the GUARDIUM_STAP service, for example:

```
--set-service GUARDIUM_STAP=restart
```

Windows: Discover database instances

The instance discovery agent runs once per day, by default. It reports new database instances, listener, and port information to the Guardium® system. It does not update the inspection engine configurations.

Instance discovery uploads its findings to the Discovered Instances report of the associated Guardium system.. You can add datasources and inspection engines to Guardium by using the Actions menu in the report.

You can modify the discovery frequency in the UI, by modifying the parameter Discovery interval in the [S-TAP Control: Details](#) page, or the DISCOVERY_INTERVAL parameter in the guard_tap.ini . For more information, see [Discovery parameters](#) or [Protocol 8 Discovery parameters](#).

You can run the database instance discovery manually in the S-TAP Control page by clicking  Send, and selecting Run Database Instance Discovery. If you start a manual discovery while a scheduled discovery is running, the new request is ignored. To avoid an instance where S-TAP discovery does not open the Informix database, it is recommended to start Informix databases by using the full path to the executable.

Important: Do not check Replace Inspection Engines unless you want to overwrite the existing inspection engine configurations.

You can define rules to manage inspection engine creation on discovered database instances. For more information, see [Database discovered instances rules](#). This configuration is used when you run the Send command in the S-TAP Control page. Do not check Replace Inspection Engines when using the rules.

Instance discovery is configured and run independently of auto discovery. For more information, see [Windows: Auto discovery of database instances during installation and upgrade](#).

Related concepts

- [S-TAP Control: Details](#)
- [Database discovered instances rules](#)

Related reference

- [Discovery parameters](#)
- [Protocol 8 Discovery parameters](#)

Windows: Configuring an Inspection Engine

Configure or modify an inspection engine in the S-TAP Control pane.

Before you begin

You must be logged in to the Guardium system that manages the S-TAP.

About this task

Do not configure an S-TAP inspection engine to monitor network traffic that is also monitored directly by a Guardium system that is hosting the S-TAP, or by another S-TAP reporting to the same Guardium system. That would cause the Guardium system to receive duplicate information: it would not be able to reconstruct sessions, and it would ignore that traffic.

You can also add inspection engines directly in the guard_tap.ini file, see [Editing the protocol 7 and protocol 8 S-TAP configuration parameters](#).

You can define up to 50 inspection engines per S-TAP.

Procedure

1. Navigate to Manage > Activity Monitoring > S-TAP Control.
2. In the row of the S-TAP, click  .
The S-TAP Configuration window opens.
3. Scroll to the bottom of the inspection engines, and click  next to Add Inspection Engine....
4. Select the protocol and enter the port range. The window refreshes with the relevant parameters, some with their default values.
5. Configure all required parameters, and click Add. If you are missing parameters, the system informs you what is missing.

Related reference

- [Inspection engine parameters](#)

Windows: Inspection engine verification

S-TAP verification confirms that the S-TAPs and their inspection engines in your environment are running and actively monitoring database activity. Understand verification, and define a schedule to regularly verify S-TAPs.

Verification checks the sniffer operation and communication between the Guardium system and the inspection engines. You can enable verification for all S-TAP clients on your system, or individual S-TAP clients, or individual inspection engines.

Verification is supported for these database types:

- Db2
- Db2 Exit (Db2 version 10)
- FTP
- Kerberos
- Mysql
- Oracle
- PostgreSQL
- Sybase
- exclude IE
- MSSQL

There are two types of verification:

Standard verification

Checks the sniffer operation, and the communication between the S-TAP and the inspection engine. During standard verification, Guardium® attempts to log in to database defined in the inspection engine with user `resutlfd`, based on the assumption that no such user exists on the target system. (If that user exists, use advanced verification instead.) Depending on the installed policy, failed login alerts might be triggered for that login attempt. Next, the verification process checks whether it can connect to the selected inspection engine on the database server. It expects to receive a response that indicates a failed login. If a different response is received, you might have to investigate further.

Some error messages from individual databases do not indicate a specific problem. For example, on several supported databases, the error code that is returned for a wrong port can also mean that the database itself is not started.

Advanced verification

Use advanced verification to avoid failed login requests, and manage individual inspection engines. During advanced verification, Guardium logs into the database that is defined in the configured datasource. It runs `select * from non_existent_table`. Depending on the installed policy, this SQL might appear in reports or alerts.

- [Windows: S-TAP verification](#)
The S-TAP verification process checks several configuration parameters and attempts to connect to the inspection engines.
- [Windows: Configure standard verification](#)
Use this task to add all inspection engines on a specific S-TAP client host to the verification schedule.
- [Windows: Configure advanced verification](#)
Use this task to run advanced verification on individual inspection engines on a specific S-TAP client host, and to add individual inspection engines to advanced verification.
- [Windows: Configuring the S-TAP verification schedule](#)
You can configure the schedule for running S-TAP verification.

Windows: S-TAP verification

The S-TAP verification process checks several configuration parameters and attempts to connect to the inspection engines.

Before connecting to the database, the verification process checks whether the sniffer process is running on the Guardium® system. The sniffer is responsible for communicating with each S-TAP and processing the data that is received. If the sniffer is not running, responses from the S-TAP are not recognized.

The verification process attempts to log in to your database's STAP client with an erroneous user ID and password, to verify that this attempt is recognized and communicated to the Guardium system.

Next the verification process checks whether it can connect to the selected inspection engine on the database server. It expects to receive a response that indicates a failed login. If a different response is received, you might have to investigate further.

Some error messages from individual databases do not indicate a specific problem. For example, on several supported databases, the error code returned for a wrong port can also mean that the database itself is not started.

Windows: Configure standard verification

Use this task to add all inspection engines on a specific S-TAP client host to the verification schedule.

About this task

As an alternative to this procedure, you can:

- Use the API command `verify_stap_inspection_engine_with_sequence`.
- Use the procedure in [Windows: Configure advanced verification](#) to configure verification on individual inspection engines, by clicking Verify in step 4. The system immediately outputs results. Failed checks are shown first, with recommendations for next steps. Checks that succeeded are shown in a collapsed section at the end of the list. In some situations, it might be useful to review the successful checks in order to choose among possible next steps.

Procedure

1. Access Manage > Activity Monitoring > S-TAP Control.
2. Use these options:
 - Add All to Schedule: add all inspection engines for all displayed S-TAPs to verification.
 - Remove All from Schedule: remove all inspection engines for all displayed S-TAPs from verification.
 - Add to Schedule: add all inspection engines of the selected S-TAP client to the schedule.If an S-TAP does not have the option All Can Control enabled, you can only change its status if your Guardium system is the primary system for this S-TAP.
3. Click Refresh.
4. To verify now, go to Manage > Activity Monitoring > S-TAP Verification Scheduler and click Run Once Now.
5. By default, the system waits five seconds before displaying verification results. If your network latency is high, this might not be enough time to receive the expected response from the database server. If you need to allow more time, you can use the `store_stap_network_latency` CLI command to change the period.

What to do next

View the verification results in the S-TAP Verification page (Manage > Reports > Activity Monitoring > S-TAP Verification page).

Windows: Configure advanced verification

Use this task to run advanced verification on individual inspection engines on a specific S-TAP client host, and to add individual inspection engines to advanced verification.

Procedure

1. Access Manage > System View > S-TAP Status Monitor.
2. Click anywhere in the row of the S-TAP.
The window refreshes with the individual inspection engines of this host.
3. To output immediate verification results, take the following steps:
 - a. Click one inspection engine, and click Advanced Verify.
 - b. 12.0 Optionally, under Datasource, select Show only matching S-TAP host or select a name from the Name list to search for a specific inspection engine.
12.1 and later Optionally, under Datasource, make sure that Show only matching S-TAP host and host is selected. If you select a datasource for which the IP address or port does not match the datasource, then an error message is returned.
 - c. Click Verify.The S-TAP Verification Results opens. Failed checks are shown first, with recommendations for next steps. Checks that succeeded are shown in a collapsed section at the end of the list. In some situations, it might be useful to review the successful checks in order to choose among possible next steps.
4. By default, the system waits five seconds before it displays verification results. If your network latency is high, five seconds might not be enough time to receive the expected response from the database server. If you need to allow more time, you can use the `store_stap_network_latency` CLI command to change the period.
5. To add to or remove individual inspection engines to the verification schedule:
 - a. Select one or more inspection engines.
 - b. Click Add to Schedule or Remove from Schedule

What to do next

View the results of schedules verification in the S-TAP Verification page (Manage > Reports > Activity Monitoring > S-TAP Verification).

Windows: Configuring the S-TAP verification schedule

You can configure the schedule for running S-TAP verification.

About this task

The same schedule is used for all S-TAPs that are scheduled for verification. Once a schedule is defined, you can click the Pause button in the S-TAP Verification Scheduler to temporarily stop the verification process while keeping it active. Use the Run Once Now button to run the verification once in real-time.

Procedure

1. Click [Manage > Activity Monitoring > S-TAP Verification Scheduler](#) to open the S-TAP Verification Scheduler.
 2. In the S-TAP Verification Scheduler portion of the page, click **Modify Schedule**.
 3. In the Schedule Definition dialog, use the drop-down lists and check boxes to schedule when verification runs.
This schedule is applied to all S-TAPs that are scheduled for verification.
 4. Click **Save** to save your changes.
-

Windows: S-TAP load balancing models and configuration guidelines

Understand the S-TAP load balancing models, and choose the one appropriate to your setup.

Failover

S-TAP sends traffic to one collector (primary) and fails over to the secondary as needed. The S-TAP agents are configured with a primary and at least one secondary collector IP. If the S-TAP agent cannot send the traffic to the primary collector, the S-TAP agent automatically fails over to the secondary. It continues to send data to the secondary host until either the secondary host system becomes unavailable, the primary host becomes available again, or until the S-TAP is restarted (at which point it attempts to connect to its primary host first). If the secondary host system becomes unavailable, it fails over to another secondary if there is one defined. In the second case S-TAP fails over from the secondary Guardium® host back to the Primary Guardium host.

Set up a primary and up to two secondary collectors. You can either define one collector as a standby failover collector only, or a few failover collectors. When you use one standby failover, one collector is usually sufficient for 4-5 collectors. When you use a few failover collectors, each one should run at a maximum 50% capacity, so that there are always resources for additional load. Choose the setup that works best with your architecture, database, and data center layout. If the primary becomes available, the S-TAP fails back from the secondary Guardium host back to the Primary Guardium host.

The S-TAP restarts each time configuration changes are applied from the active host.

1. In the Details section of the S-TAP Control window, set the value of the Load balancing parameter to 0; In the **Guardium Hosts** section: add at least one secondary Guardium Host.
Note: If you are not an advanced user, do not update the default failover configuration default values.
2. Before designating a Guardium system as a secondary host for an S-TAP, verify these items.
 - The Guardium system must have connectivity to the database server where S-TAP is installed. When multiple Guardium systems are used, they are often attached to disjointed branches of the network.
 - The Guardium system must not have a security policy that will ignore session data from the database server where S-TAP is installed. In many cases, a Guardium security policy is built to focus on a narrow subset of the observable database traffic, ignoring all other sessions. Either make sure that the secondary host will not ignore session data from S-TAP or modify the security policy on the Guardium system as necessary.

Enhanced failover mechanism to avoid data loss

12.1 and later

The main goal of failover mechanism is to preserve the session parameters when switching the S-TAP to the secondary collector. The regular failover mechanism saves session parameters in the form of failover messages that are received from the primary collector over the network. If a failover occurs, the mechanism forwards the failover messages to the secondary collector. In rare cases, the failover messages are lost. To address this, the enhanced failover mechanism, also saves session parameters in the form of several raw database protocol packets. If a failover is required and the failover messages are lost, the failover mechanism forwards the raw database packets to the secondary collector.

Load Balancing

This configuration balances traffic from one database onto multiple collectors. This option is useful when you must monitor all traffic (comprehensive monitoring) of an active database. (Note that for outliers detection, the collectors must be under the same aggregator and central manager in order for the aggregator to process all related data.) When the generated traffic is large and you need to house the data online on a collector for an extended period, use this method because it performs session-based load balancing across multiple collectors. An S-TAP can be configured in this manner with up to 10 collectors.

Complete the following configuration procedure in the Details section of the S-TAP Control window:

- Set the value of the Load balancing parameter to 1 for balancing the load.

Internal load balancing

12.1 and later

The Internal Load Balancer (ILB) helps avoid data loss caused due to collector overload.

The ILB evaluates the data load and helps avoid the data loss by proactively forecasting the load on the collector and redirecting the traffic to another collector to balance this load.

On the sniffer, ILB dynamically determines the number of sessions that a sniffer can accept from the S-TAP. This value is based on the collector's capacity for session information and processing collector load.

ILB sends two values to the S-TAP: the total number of allowed sessions on the appliance and the total number of sessions currently opened in the sniffer.

Note: The calculation of current sessions includes all the connected S-TAPs.

Each S-TAP keeps count of open sessions and uses the allowed session count to determine whether it can send new session data to the existing collector.

If number of open sessions is more than the allowed session count, then the S-TAP redirects new sessions to another collector.

If the number of open sessions do not exceed the allowed session count then the S-TAP may send the new sessions to existing collector.

Enabling internal load balancer

12.1 and later

Enabling on Windows

1. To enable the internal load balancer feature on S-TAP, set the INTERNAL_LOAD_BALANCER_ENABLED parameter to 1 . Default value = 0. Value range = 0, 1.
2. Also, set the PARTICIPATE_IN_LOAD_BALANCING to 1 for Windows.
Default value = 0. Valid values = 0 - 3.

Enabling on Collector

1. Create a session-level policy. For more information on creating session-level policy, see [Creating session-level policies](#).
2. In the Rule action field, select CONFIGURE.
3. In the Option field, select ILB and click OK.

Grid

With Grid, the S-TAP communicates to the collector through a load balancer, such as f5 and Cisco. The S-TAP agent is configured to send traffic to the load balancer. The load balancer forwards the S-TAP traffic to one of the collectors in the pool of collectors. You also can configure failover between load balancers for continuous monitoring if the load balancer should fail.

The persistence of S-TAP is configured by the failover parameters:

- TAP_MIN_TIME_BEFOREFAILOVER: The time interval, in minutes, after which the S-TAP switches to secondary Guardium system if: it cannot connect to its primary Guardium system; it can connect to its primary Guardium system but cannot write to its buffer. Default is 5.
- TAP_MIN_HEARTBEAT_INTERVAL: Maximum time the S-TAP attempts to write to the primary Guardium system buffer before attempting to write to the secondary Guardium buffer. Default is 30 sec, meaning it tries to write at least 5*60/30 times before failover.

S-TAPs in the F5 environment upload their log files and results of running diagnostics (all files from ..\Logs folder except for memory dumps) to the active collector and central manager (if exists) to the location ./var/IBM/Guardium/log/stap_diagnostic/

1. In the Details section of the S-TAP Control window, set the value of the Load balancing parameter to 3 for the grid model.
2. All can control = 1.
3. Guardium Host = <the IP of the Virtual IP of the balancer, to which all S-TAP database clients point to>.

Redundancy

In redundancy, the S-TAP communicates its entire payload to multiple collectors. The S-TAP is configured with more than one collector (often only two) and communicates the identical content to both. This option provides full redundancy of the same logged data across multiple collectors. It can also be used for logging data and alert on activity at different levels of granularity.

In the Details section of the S-TAP Control window, set the Value of the Load balancing parameter to 2 for redundancy. For more information, see [S-TAP Control: Details](#).

Windows: Configuring the Db2 Exit library

The Db2 Exit mechanism enables Guardium to pick up all Db2 traffic, whether encrypted or not and whether local or remote. This solution simplifies the S-TAP configuration, and provides native Db2 support.

About this task

Db2 Exit embeds a Guardium library into Db2 by using the Db2 Exit mechanism. The Db2 Exit communicates directly with the Guardium S-TAP to forward all Db2 traffic, whether encrypted or not, and both local and remote. Db2 Exit captures TCP and SHM traffic.

Db2 Exit supports terminate.

The guard_tap.ini DB2_PROTOCOLS and WINSTAP_DB2_PROTOCOLS GIM parameters specify the protocols that the Db2 Exit picks up.

- For unencrypted TCPIP traffic, you can use the default value, which is `LOCAL,PIPES,SSL` (with no spaces between values). In this case, TCPIP traffic is picked up from the WFP Monitor driver. However, WFP Monitor ignores encrypted traffic.
- For encrypted TCPIP traffic, include the `TCPIP` parameter to DB2_PROTOCOLS to allow TCPIP to pick up the encrypted traffic, for example:

`DB2_PROTOCOLS=LOCAL,PIPES,SSL,TCPIP`

Limitations

- Db2 Exit does not support the firewall, redact, or query rewrite functions.
- If you add `TCPIP` to DB2_PROTOCOLS, Db2 Exit captures TCPIP traffic in all ports. In this case, you do not need to specify PORT_RANGE_START and PORT_RANGE_END in the Db2 Exit inspection engine.
However, if you do not specify `TCPIP` in DB2_PROTOCOLS, the WFPMonitor driver picks up TCP traffic. In this case, the WFPMonitor driver refers to PORT_RANGE_START and PORT_RANGE_END in the Db2 exit inspection engine.

Procedure

1. Create a folder within the Db2 SQLLIB folder, for each instance: \$DB2PATH\security\plugin\commexit\instance_name. For example, C:\Program Files\IBM\SQLLIB\security\plugin\commexit\DB2_01
2. Copy the corresponding DLLs from the S-TAP installation directory into the created directories:
 - For 32-bit Db2 - GuardiumInterfacex86.dll
 - For 64-bit Db2 - GuardiumInterfacex64.dll
3. Stop the Db2 instance, or instances, and issue the following command:

- For 32 bit - UPDATE DBM CFG USING COMM_EXIT_LIST GuardiumInterfaceX86
 - For 64 bit - UPDATE DBM CFG USING COMM_EXIT_LIST GuardiumInterfaceX
4. Start the Db2 instances.
5. Add an inspection engine for Db2 Exit with protocol Db2 Exit. Go to Manage > Activity Monitoring > S-TAP Control. See parameter descriptions in [Inspection engine parameters](#). Advanced users can also modify the guard_tap.ini, but it's best to use the GUI since it completes some of the information automatically, and does some validation. If you modify the guard_tap.ini file, set these parameters:
- [DB_DB2_EXIT1]
 - DB_TYPE=DB2_EXIT
 - INSTANCE_NAME=Service_name
- In the TAP section, set the parameter DB2_EXIT_DRIVER_INSTALLED=1
- The service name is not the instance name. You can determine the service name by using the db2tap utility in the S-TAP installation folder, or from the Control Panel. Set the instance name to the portion of the service name that follows the second dash (-) delimiter. For example, if the service name in the Control Panel is DB2 - DB2COPY1 - DB2-01-0, set INSTANCE_NAME to DB2-01-0.
6. To stop Db2 Exit, issue the following command, and then restart Db2:
- ```
db2 UPDATE DBM CFG USING COMM_EXIT_LIST NULL
```

## Windows: Upload dump files from the S-TAP to the collector and central manager

You can configure the S-TAP to automatically upload dump files upon restart, to the collector and the central manager, or only the collector.

The guard\_tap.ini parameter **upload\_feature** controls this upload feature:

- 0: No automatic upload.
- 1: Upload files to the collector and the central manager.
- 2: Upload files **only to the collector**, even if there is a central manager.

If enabled, when the S-TAP restarts, and it detects a new dump file in one of the monitored folders, it:

1. Collects all of the information (dump file, log files, etc.) from Program Files\IBM\Windows S-TAP\Logs.
2. Compresses the files.
3. Uploads the .zip file to the collector and/or central manager, to the folder /var/IBM/Guardium/log/stap\_diagnostic.

The .zip file name is in the format: WSTAP\_<computer name>\_<ISO time of file creation>.zip

The files on the collector are purged to prevent excessive disk space usage. If the total space used is greater than 10 GB, the oldest files are purged to bring the size down to less than 10 GB. Files older than one month are purged, irrelevant of the disk space used. Only the files in /var/IBM/Guardium/log/stap\_diagnostic are purged.

If the upload of a .zip file would result in /var going over 70%, then the .zip file is not uploaded.

For an S-TAP that was installed with GIM, the GIM server uses the threshold2 value defined in **Utilization\_Threshold** for System Var Disk Usage, which is 70% by default. If the file to upload would result in system var disk usage over the threshold2 value, the upload is rejected. You can modify this value. See [update\\_utilization\\_thresholds](#).

## Related reference

- [list\\_utilization\\_thresholds](#)
- [update\\_utilization\\_thresholds](#)

## Windows: Build and configure FreeTDS for Guardium

FreeTDS allows Unix/Linux machines to connect to an SQL Server on Windows machines.

### Before you begin

Verify these requirements for using FreeTDS successfully with Guardium®, such that all information (DB\_USER, SOURCE\_PROGRAM, etc.) is included in the Guardium reports.

- FreeTDS V1.00.111 or later
- OpenSSL Support in FreeTDS
- Kerberos Support in FreeTDS
- TDS Version Auto in FreeTDS
- Domain Joined Linux System
- Domain Joined SQL Server Windows System Setup for Kerberos Logins

### About this task

To determine what version of FreeTDS you have and what type of support has been compiled into the program, execute the command **tsql -C** to see the FreeTDS characteristics on your machine. You should see something like:

```

Compile-time settings (established with the "configure" script)
 Version: freetds v1.00.111
 freetds.conf directory: /usr/local/etc
 MS db-lib source compatibility: no
 Sybase binary compatibility: no
 Thread safety: yes
 iconv library: yes
 TDS version: auto
 iODBC: no
 unixodbc: no
 SSPI "trusted" logins: no
 Kerberos: yes
 OpenSSL: yes
 GnuTLS: no
 MARS: no

```

## Procedure

1. Download a suitable C/C++ compiler package and an OpenSSL package. See instructions in the users guide [www.freetds.org](http://www.freetds.org) for more details and for the download of the latest FreeTDS package.
2. Unpack the tarball and then set your folder to the FreeTDS kit root folder. Enter the following commands:

```

$./configure --enable-krb5 --with-openssl
$ make
$ su root
Password
$ make install

```

3. Test that the SQL Server logs in to a system named “node” and determine whether Kerberos is being used. Enter the commands:

```

$ tsql -S node
1> select auth_scheme from sys.dm_exec_connections where session_id = @@SPID
2> go
auth_scheme
KERBEROS
(1 row affected)

```

## Windows: S-TAP configuration per database type

This section provides detailed instructions or examples for configuring monitoring on various databases.

- [Windows: Db2 configuration for SSL](#)  
Db2 configuration for SSL requires the following parameters in the guard\_tap.ini.

## Windows: Db2 configuration for SSL

Db2 configuration for SSL requires the following parameters in the guard\_tap.ini.

- DB2\_EXIT\_DRIVER\_INSTALLED=0
- DB2\_SSL\_DRIVER\_INSTALLED=1
- DB2\_TAP\_INSTALLED=0

The Db2 service needs to be restarted following the S-TAP configuration, to inject the DB2 SSL library.

## Windows: S-TAP operation and performance

- [Windows: Stopping S-TAP using GIM](#)  
With GIM, you can stop S-TAP without logging into the database server.
- [Windows: Starting S-TAP using GIM](#)  
With GIM, you can start S-TAP without logging into the database server.
- [Windows: Starting S-TAP without GIM](#)  
Learn to start S-TAP from the database server.
- [Windows: Stopping S-TAP without GIM](#)  
Learn to stop S-TAP from the database server.
- [Windows: Multi-threading S-TAP for increased throughput](#)  
S-TAP multi-threading can be used in certain workloads to increase the throughput of data in the S-TAP. It works by preserving multiple threads from the point of traffic interception through to the point at which traffic is sent to the collector.
- [Windows: Capturing encrypted MSSQL traffic](#)  
Understand the correlation driver that is used for capturing encrypted MSSQL traffic.
- [Windows: Alerts on uninstalled S-TAPs](#)  
Uninstalling an S-TAP might be evidence of harmful activity. The predefined S-TAP Uninstall Alert notifies when an S-TAP is uninstalled. You can view the S-TAP Uninstall Events report in My Dashboards.
- [Windows: Deleting inactive S-TAPs in a centralized environment](#)  
You can use a cron job on the central manager to delete all inactive S-TAP instances.

- [Windows: Monitoring S-TAP in the GUI](#)  
Use these standard reports and views to monitor your S-TAP status in the GUI.
- [Windows: Log and debug files](#)  
The S-TAP can create log and debug files. The files are located in the logs directory under the installation directory.
- [Windows: S-TAP statistics](#)  
The S-TAP statistics are sent by the S-TAP to the sniffer are stored on the collector. You can see the statistics in the predefined S-TAP Statistics report.
- [Windows: Monitoring with the Guardium Agent Monitor](#)  
The Guardium Agent Monitor (GAM) process monitors Guardium agent performance and responsiveness. Use GAM for detailed analysis during troubleshooting.
- [Windows: Troubleshooting S-TAP problems](#)  
You can use the S-TAP Status monitor tab of the System View to begin investigating any problems. Sometimes you might need to use other tools, particularly if you are monitoring databases for which the inspection engines cannot be verified.

## Windows: Stopping S-TAP using GIM

With GIM, you can stop S-TAP without logging into the database server.

### About this task

Use the following steps to change the WINSTAP\_ENABLED parameter and schedule the S-TAP startup on the database server.

### Procedure

1. Navigate to Manage > Module Installation > Set up by Client.
2. In the Choose clients section, select the database servers whose S-TAPs you want to stop. Select individual clients using check boxes in the table, or use the Select client group menu to select a group of clients. Click Next to continue.
3. In the Choose bundle section, select your S-TAP bundle. Click Next.  
After selecting a software bundle, the Selected bundle action column indicates the action that will be performed for each client. You can stop the S-TAPs that have the status Update parameters.
4. In the Choose parameters section, type WINSTAP\_ENABLED and type in the value 0. Click Next.
5. In the Configure clients section, use the table to review the changes you want to make.
6. Click Install.
7. Click OK to stop the S-TAP now, or use the  icon to schedule the stop time, then click OK.

## Windows: Starting S-TAP using GIM

With GIM, you can start S-TAP without logging into the database server.

### About this task

Use the following steps to change the WINSTAP\_ENABLED parameter and schedule the S-TAP startup on the database server.

### Procedure

1. Navigate to Manage > Module Installation > Set up by Client.
2. In the Choose clients section, select the database servers whose S-TAPs you want to start. Select individual clients using check boxes in the table, or use the Select client group menu to select a group of clients. Click Next to continue.
3. In the Choose bundle section, select your S-TAP bundle. Click Next.  
After selecting a software bundle, the Selected bundle action column indicates the action that will be performed for each client. You can start the S-TAPs that have the status Update parameters.
4. In the Choose parameters section, type WINSTAP\_ENABLED and type in the value 1. Click Next.
5. In the Configure clients section, use the table to review the changes you want to make.
6. Click Install.
7. Click OK to start the S-TAP now, or use the  icon to schedule the start time, then click OK.

## Windows: Starting S-TAP without GIM

Learn to start S-TAP from the database server.

### About this task

Note: When Windows S-TAP encounters a fatal error during start up that is due to configuration problems (unknown local IP address, more than 1 primary SQL-Guard defined, etc.) it logs the reason to the Windows event log. In some cases an exit after a failure may cause a crash and another logged event. This crash should not cause any concern if it is preceded by the event explaining the reason for the failure.

### Procedure

1. Log on to the database server system using a system administrator account.

2. From the Services control panel, start the IBM Security Guardium S-TAP.
3. Log in to the Guardium® system to which this S-TAP reports. Verify that the Status light in the S-TAP control panel is green.

## Windows: Stopping S-TAP without GIM

Learn to stop S-TAP from the database server.

### Procedure

1. Log on to the database server system using a system administrator account.
2. From the Services control panel, stop the IBM Security Guardium S-TAP.
3. Log in to the UI of the Guardium® system to which this S-TAP was reporting, verify that the Status light in the S-TAP control panel is now red.

## Windows: Multi-threading S-TAP for increased throughput

S-TAP multi-threading can be used in certain workloads to increase the throughput of data in the S-TAP. It works by preserving multiple threads from the point of traffic interception through to the point at which traffic is sent to the collector.

If the S-TAP is dropping a lot of traffic, or if there is evidence that intercepting the traffic is impacting the database performance, then you might consider enabling multiple S-TAP threads. An increased number of S-TAP threads means that the S-TAP increases its throughput to the collectors. But it also means that S-TAP might use more CPU and more memory. Multi-threading does not rectify a slow or busy network.

There are no definitive rules, you first modify the configuration, then fine-tune the results. The S-TAP has a maximum of 8 connections to each of its collectors.

When one or more Guardium® systems can not be reached, a failover mechanism redirects the traffic from one Guardium system to another.

### Limitations

- Multi-threading is supported only for the TCP/IP and Named Pipes protocols. Multi-threading is supported on any platform but only for those protocols.
- Policies have to be the same on all Guardium system because the policies dictate what happens to a system's traffic. If the policies are different, there's no guarantee which policy is in effect on a given session.
- Multi-threading S-TAP requires V11.3 **Protocol 8**. It is not available in V11.3 Protocol 7. To enable Protocol 8, in the TAP section of the guard\_tap.ini, set the parameter V8\_PROTOCOL=1.

## Configuration Guidelines

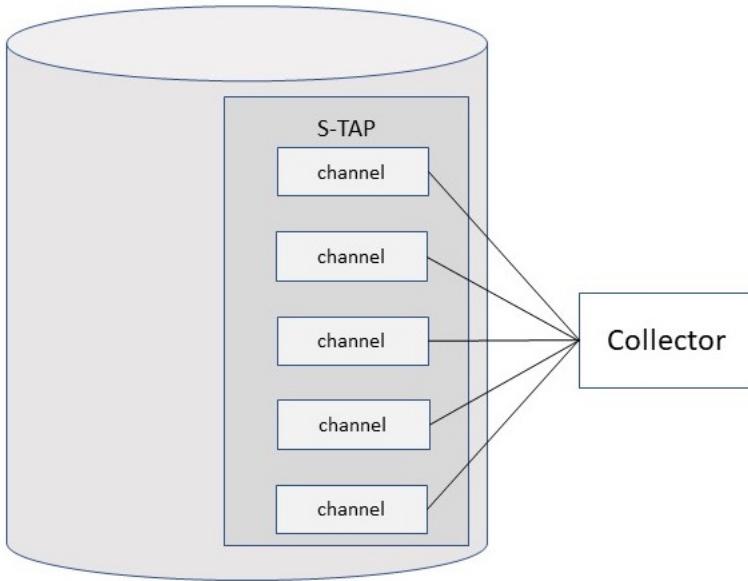
The parameter TCP\_CHANNELS in the TAP section of the guard\_tap.ini file determines the number of channels to each collector. It affects all collectors defined in the guard\_tap.ini file.

### Implementing multi-threading or increasing the number of threads

Set or increase the TCP\_CHANNELS parameter in the corresponding TAP section.

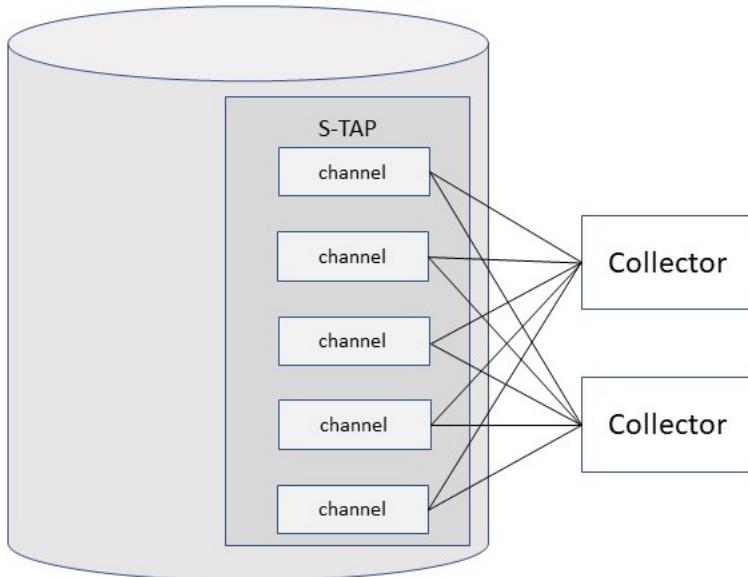
### Example: One collector, five threads

```
[TAP]
...
TCP_CHANNELS=5
[SQLGUARD_1]
SQLGUARD_IP=n.n.n.n
PRIMARY=1
```



## Example: Two collectors, five threads

```
[TAP]
...
TCP_CHANNELS=5
[SQLGUARD_1]
SQLGUARD_IP=n.n.n.n
PRIMARY=1
[SQLGUARD_2]
SQLGUARD_IP=n.n.n.n
PRIMARY=2
```



## Related concepts

- [Windows: S-TAP statistics](#)

## Windows: Capturing encrypted MSSQL traffic

Understand the correlation driver that is used for capturing encrypted MSSQL traffic.

The correlation driver facilitates the communications between the Guardium® DLLs that are injected into the SQL Server Process and the Guardium traffic drivers (WFP, NMP). The Guardium DLLs get the encryption key used by the S-TAP to decrypt the SQL Server traffic, but the DLLs do not know which session (IPs, ports) that the encryption key belongs to. The correlator driver matches the encryption key to the session in the traffic drivers (WFP, NMP) so that the DLLs can then apply the proper key to the proper session. Finally, the DLLs supply the encryption key to the proper session in the traffic drivers that use the correlation driver so the traffic drivers can deliver the encryption key to the S-TAP. The S-TAP uses the encryption key to decrypt the SQL Server traffic for the session and sends it to the appliance.

The correlation DLLs in an SQL Server depend on the correlation driver, which depends on the traffic drivers (WFP, NMP). Without either the correlation DLLs or the correlation driver, Guardium cannot decrypt traffic. In all cases, the login packet for an SQL Server session is always encrypted. Missing or malfunctioning correlation DLLs or driver results in sessions that are missing their DB username, source program, and a few other fields. If the entire session is encrypted, and the correlation DLLs or the driver are missing or malfunctioning, then no traffic for this session reaches the collector.

The S-TAP holds traffic back for a session until it receives the encryption key. After it receives the encryption key, it decrypts the traffic it's holding and releases it to the appliance. It then decrypts any subsequent traffic and sends that to the appliance as well. However, if the encryption key does not show up before the `guard_tap.ini` parameter `CORRELATION_TIMEOUT` threshold, then the S-TAP gives up and sends the traffic to Guardium as is. In that case, for unencrypted traffic, the sessions are missing DB username, source program, and other fields. With fully encrypted traffic, no traffic is seen.

## Related reference

---

- [General parameters](#)
  - [Protocol 8 General parameters](#)
- 

## Windows: Alerts on uninstalled S-TAPs

---

Uninstalling an S-TAP might be evidence of harmful activity. The predefined S-TAP Uninstall Alert notifies when an S-TAP is uninstalled. You can view the S-TAP Uninstall Events report in My Dashboards.

By default the alert is scheduled hourly. View and optionally configure the Alert Receivers in the Alert Builder: Protect > Database Intrusion Detection > Alert Builder. Tip: Best practice is to leave the alert settings at their defaults. If you need to change the configuration, run the CLI command `restart gui` so that the changes take effect. The alert writes to SYSLOG in the format: Alert Name: STAP Uninstall Alert. Alert Description: STAP Uninstall Alert... ...<S-TAP host>. The S-TAP host uniquely identifies the S-TAP. It is usually the database IP.

## Related concepts

---

- [Predefined alerts](#)
- 

## Windows: Deleting inactive S-TAPs in a centralized environment

---

You can use a cron job on the central manager to delete all inactive S-TAP instances.

## Procedure

---

1. Go to Manage > System View > Enterprise S-TAP View.
2. In the Actions menu, select Add API mapping.
3. In the Add API Mapping dialog, search for and select `delete_inactive_stap`.
4. In the Enterprise S-TAP view, right-click in any row and select Invoke > `delete_inactive_stap`
5. Create a script to schedule running this API periodically on the central manager.

Sample shell script for running the API:

```
#!/bin/bash

echo >> ${GUARD_LOG_DIR}/delete_inactive_staps.log
echo >> ${GUARD_LOG_DIR}/delete_inactive_staps.log

echo Deleting inactive staps from all managed units $dateStr >> ${GUARD_LOG_DIR}/delete_inactive_staps.log
date >> ${GUARD_LOG_DIR}/delete_inactive_staps.log

#Run the delete inactive stap command from CM for all S-TAPs on all managed_units

echo -e "grdapi delete_inactive_stap stapHost=all api_target_host=all_managed" | su - cli >>
${GUARD_LOG_DIR}/delete_inactive_staps.log

exit 0
```

6. Create a cron job to run the script after the report is refreshed, at whatever interval you decide for both the report refresh and the cron job.

## Related reference

---

- [delete\\_inactive\\_stap](#)
- 

## Windows: Monitoring S-TAP in the GUI

---

Use these standard reports and views to monitor your S-TAP status in the GUI.

You can create alerts that are based on exceptions that are created by S-TAPs, but other domains that are used by S-TAP reports are system-private and cannot be accessed by users.

## System View

---

**S-TAP Status Monitor** in the System Monitor window: For each S-TAP reporting to this Guardium® system, this report identifies the S-TAP Host, S-TAP Version, DB Server Type, Status (active or inactive), Last Response Received (date and time), Instance Name, Primary Host Name, and true/false indicators for: MS SQL Server Shared Memory, DB2® Shared Memory, Win TCP, Local TCP monitoring, Named Pipes Usage, Encryption, Firewall, DB install Dir, DB port Min and DB Port Max.

Click any line to view the inspection engines that are configured for this S-TAP. The bread crumbs show where you are; click ALL S-TAPs to return to the list of S-TAP. For more details, see [Windows: Inspection engine verification](#).

**S-TAP Status Monitor:** For each S-TAP reporting to this Guardium system, this report identifies the S-TAP Host, DB Server Type, S-TAP Version, Status (active or inactive), Inspection Engine status, Last Response Received (date and time), Primary Host Name, and true/false indicators for: Firewall and Encrypted. Click the S-TAP Status and the Inspection Engine status to see the Verification status on all Inspection Engines.

**S-TAP Events:** For each S-TAP reporting to this Guardium system, this report identifies the S-TAP Host, Timestamp, Event type (Success, Error Type, and so on), and Tap Message.

If no messages display in the S-TAP Events panel, the production of event messages may have been disabled in the configuration file for that S-TAP. If this is the case, you may be able to locate S-TAP event messages on the host system in the Event Log.

## Tap Monitor

**Primary Guardium Host Change Log:** Log of primary host changes for S-TAPs. The primary host is the Guardium system to which the S-TAP sends data. Each line of the report lists the S-TAP Host, Guardium Host Name, Period Start, and Period End.

**S-TAP Status:** Displays status information about each inspection engine that is defined on each S-TAP Host. This report does not have From and To date parameters, since it is reporting current status. Each row of the report lists the S-TAP Host, DB Server Type, Status, Last Response, Primary Host Name, Yes/No indicators for the following attributes: Shared Memory Driver Installed, Db2 Shared Memory Driver Installed, Named Pipes Driver Installed, and App Server Installed. In addition, it lists the Hunter DBS.

**Inactive S-TAPs Since:** Lists all inactive S-TAPs that are defined on the system. It has a single runtime parameter: QUERY\_FROM\_DATE, which is set to now -1 hour by default. Use this parameter to control how you want to define *inactive*. This report contains the same columns of data as the S-TAP Status report, with the addition of a count for each row of the report.

## Windows: Log and debug files

The S-TAP can create log and debug files. The files are located in the logs directory under the installation directory.

## Protocol 8

### Debug files

Debug is disabled by default. The guard\_tap.ini parameter DEBUGLEVEL enables debug and controls the level. See [Protocol 8 Debug parameters](#).

The debug log is STAP.CTL and is located in the logs directory, under the installation directory.

The debug log is exclusively for logging all telemetry and status information. You can view these files using Notepad.

The following guard\_tap.ini parameters control what gets logged to the STAP.CTL log file and how verbose it is.

- LOG\_WFP\_CONNECTIONS: the particular protocol's status information. The default is 0, which means that is not logged to the STAP.CTL file. A value of 1 logs things like connection establishment, connection termination, and a few others for the protocol in question.
- LOG\_NMP\_CONNECTIONS: same as LOG\_WFP\_CONNECTIONS
- LOG\_DB2\_CONNECTIONS: same as LOG\_WFP\_CONNECTIONS
- LOG\_INFORMIX\_CONNECTIONS: same as LOG\_WFP\_CONNECTIONS
- LOG\_ORA\_CONNECTIONS: same as LOG\_WFP\_CONNECTIONS
- LOG\_LEVEL: The verbosity of the overall logging of the S-TAP output to the Stap.ctl circular text log file. The default is 4, and it ranges from 0 to 10. The higher the number, the more verbose the logging.
- KERNEL\_DEBUG\_LEVEL: The verbosity of the overall logging for the driver-based .CTL files.

Auto discover debug messages are also logged in stap.ctl. Each [AD<dbtype>] has logs of the indicated DB type. Logs include step-by-step success or failure discovery of instance names, process names, ports, named pipes, and so on. Examples:

```
`I 05/10/2020 14:46:34.917 ADmssql: Start discovering 64-bit instances.
`W 05/10/2020 14:46:34.917 ADmssql: Registry path not found: SOFTWARE\Wow6432Node\Microsoft\Microsoft SQL Server\Instance Names\SQL
`I 05/10/2020 14:46:34.917 ADoracle: Start discovering
```

### Traffic debug log

The traffic log is a file with a .txt extension in the Logs directory, under the installation directory. You can initiate traffic logging in two ways.

- From the collector, trigger traffic collection, for up to 4 minutes of S-TAP traffic. Click Send Command, and select S-TAP logging in the S-TAP Control page. For more information, see [Send command](#).
- From the database server, change the DEBUGLEVEL parameter to a non-zero value in the .INI file. The S-TAP creates a recording of traffic in binary format. When you set it back to 0, it is converted into human readable form. The V8 S-TAP can detect .ini parameter changes without having to be restarted, so you can change the DEBUGLEVEL parameter back to 0 in the .ini file without restarting the S-TAP.

Both methods create a traffic debug log file in the S-TAP Logs folder. While traffic is being recorded, the size of the traffic file remains at 0 bytes, which is normal. When the traffic collection ceases, either because the time interval elapsed or because you changed the DEBUGLEVEL parameter back to 0, the S-TAP converts the recorded binary traffic into human readable form. As this happens, the size of the traffic file grows if you're watching it in Explorer. You need to wait until the size of the file stops increasing before you access the file and copy it off to another system. DO NOT stop the S-TAP during either traffic recording or traffic conversion, or you'll lose all the traffic that you recorded. The S-TAP automatically waits for the conversion to be completed before shipping the traffic log file to the collector when the collection of traffic is triggered from the collector itself.

## Protocol 7

---

Debug is disabled by default. The guard\_tap.ini parameter DEBUGLEVEL enables debug and controls the level. See [Debug parameters](#).

Logs and debug logs are in the bin/stap\_buffer/ folder.

Auto discover debug messages are logged in logs/Stap.ctl. Each **[AD<dbtype>]** has logs pf the indicated DB type . Logs include step-by-step success or failure discovery of instance names, process names, ports, named pipes, and so on. Examples:

```
`I 05/10/2020 14:46:34.917 ADmssql: Start discovering 64-bit instances.
`W 05/10/2020 14:46:34.917 ADmssql: Registry path not found: SOFTWARE\Wow6432Node\Microsoft\Microsoft SQL Server\Instance Names\SQL
`I 05/10/2020 14:46:34.917 ADoracle: Start discovering
```

---

## Windows: S-TAP statistics

The S-TAP statistics are sent by the S-TAP to the sniffer are stored on the collector. You can see the statistics in the predefined S-TAP Statistics report.

You can create alerts based on results.

The guard\_tap.ini parameter STAP\_STATISTIC specifies the interval at which the S-TAP sends statistics to the sniffer. Valid values are:

- Positive integer: for hours
- Negative integer: minutes
- 0: do not send

The default is -5. This is also the minimum.

S-TAP counters:

- Total dropped packets: Packets dropped due to insufficient buffer space in the S-TAP service.
- Total dropped bytes: Bytes dropped due to insufficient buffer space in the S-TAP service.
- Collector count
- Collector names: Comma-separated list of all the collectors that are assigned to the S-TAP
- Collector total dropped packets: Comma-separated list of the packets that are dropped due to insufficient buffer space in the S-TAP, cataloged by collector.
- Collector total dropped bytes: Comma-separated list of the bytes that are dropped due to insufficient buffer space in the S-TAP, cataloged by collector.

NMP counters:

- Software TAP Host
- Tap name (driver name)
- Tap version
- Timestamp
- Total packets: Total packets that pass through the driver
- Total bytes: Total bytes that pass through the driver
- Total dropped packets: Total packets that are dropped due to insufficient buffer space in the driver.
- Total dropped bytes: Total bytes that are dropped due to insufficient buffer space in the driver.
- Total ignored packets: Total packets that are ignored due to Ignore commands from the appliance or priority queue transitions.
- Total ignored bytes: Total bytes that are ignored due to Ignore commands from the appliance or priority queue transitions.
- Total ignored reply packets: Total packets of server reply data that is ignored due to ignore reply commands from the appliance, DB ignore bypass, or priority queue transitions.
- Total ignored reply bytes: Total bytes of server reply data that is ignored due to ignore reply commands from the appliance, DB ignore bypass, or priority queue transitions.

WFP counters:

- Software TAP Host
- Tap name (driver name)
- Tap version
- Timestamp
- Total packets: Total packets that pass through the driver
- Total bytes: Total bytes that pass through the driver
- Total dropped packets: Total packets that are dropped due to insufficient buffer space in the driver.
- Total dropped bytes: Total bytes that are dropped due to insufficient buffer space in the driver.
- Total ignored packets: Total packets that are ignored due to Ignore commands from the appliance or priority queue transitions.
- Total ignored bytes: Total bytes that are ignored due to Ignore commands from the appliance or priority queue transitions.
- Total ignored reply packets: Totals of server reply data that is ignored due to ignore reply commands from the appliance, DB ignore bypass, or priority queue transitions.
- Total ignored reply bytes: Totals of server reply data that is ignored due to ignore reply commands from the appliance, DB ignore bypass, or priority queue transitions.

## Windows: Monitoring with the Guardium Agent Monitor

---

The Guardium Agent Monitor (GAM) process monitors Guardium agent performance and responsiveness. Use GAM for detailed analysis during troubleshooting.

Note: Set the GAM service to off by default as it requires configuration specific to the environment in which it is installed. Improper configuration can cause serious operational issues. GAM is a tool to aid in troubleshooting and otherwise is not required.

Monitoring covers the following services:

- CPU usage

- Memory
- Handles
- Number of threads
- Alive

If a monitored agent exceeds a configured threshold, or if it does not respond to the console request, the following actions can be taken, in any combination:

- Automatically run **diag.bat** (or the name of your diagnostics application file).
- Automatically stop or restart the service..
- Automatically perform a core dump.

Guardium Agent Monitor is installed when S-TAP is installed but is not enabled by default. When S-TAP is uninstalled, GAM is uninstalled.

Note: Just like S-TAP, GAM requires administrative privileges. When you install GAM, run with "Run as Administrator" as an administrative user. If you run it as a non-admin user, GAM returns an **Access Denied** error.

The default installation location for GAM is the parent folder of S-TAP (C:\Program Files\IBM\Guardium Agent Monitor).

The default location for GAM output is the \Bin\ subfolder.

After you enable GAM, make sure that the process is running on the database server (resmon.exe).

Guardium Activity Monitor (GAM) is listed in the Services as IBM Security Guardium Resource Monitor Service, which has a Service Name property of Guardium Resource Monitor.

For an example of how GAM works, see [Resource monitoring example](#).

## Global level configuration

The following parameters pertain to the GAM service process and defined in [Global] section.

| resmon.ini          | Default value | Description                                                                                                                                                                                                                                                 |
|---------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NUMBER_OF_SERVICES  | 1             | Number of services being monitored. The minimum is 0, there is no maximum.                                                                                                                                                                                  |
| UPDATE_INTERVAL     | 1             | The length, in seconds, of the interval between polling metrics.                                                                                                                                                                                            |
| DEBUG               | 1             | Deprecated.                                                                                                                                                                                                                                                 |
| NUMBER_BYTES_IN_LOG | 200           | Maximum number of KB for the GAM log. There is no maximum size.                                                                                                                                                                                             |
| ACTION              | 1             | Determine whether to generate a dump when your system exceeds certain thresholds such as THREAD_COUNT_LIMIT or MEM_USAGE_LIMIT. Valid values: <ul style="list-style-type: none"> <li>• 0: Do not generate a dump.</li> <li>• 1: Generate a dump.</li> </ul> |
| FULLDUMP            | 0             | Valid values: <ul style="list-style-type: none"> <li>• 0: Generate a mini-dump.</li> <li>• 1: Generate a full dump when dump is generated.</li> </ul> Note: A full dump takes more time.                                                                    |
| CPUAVE              | 1             | Defines the way to calculate the average CPU time. <ul style="list-style-type: none"> <li>• 0: Percentage of one core.</li> <li>• 1: Average percentage of all cores in system.</li> </ul>                                                                  |
| MDTIMEOUT           | 1000          | Timeout of generating a dump in milliseconds. A dump is not generated if the time is exceeded.                                                                                                                                                              |

## Service level configuration

The following parameters apply to each service and are defined in the [Service\_N] section. The name of the section can be anything except [Global]. For [Service1], Name=GUARD\_STAP is defined by default.

| resmon.ini         | Default value | Description                                                                                                                                                                                                                           |
|--------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name               | GUARDIUM_STAP | The name of the Windows Service for GAM to monitor.                                                                                                                                                                                   |
| NAMEDPIPE_INTERVAL | 30            | For supported Windows S-TAPS only. The interval, in seconds, to check aliveness (supported agents only). Set to 0 to disable.<br>For more information about named pipes, see <a href="#">Inspection engine parameters</a> .           |
| DIAGACTION         | 0             | Run diagnostic on action. <ul style="list-style-type: none"> <li>• 0: Do not run diagnostics.</li> <li>• 1: Run diagnostics (usually <b>diag.bat</b>) when the monitored service exceeds the limit in specified intervals.</li> </ul> |
| DIAGNAME           | diag.bat      | Diagnostic file name. When set to <b>diag.bat</b> , GAM calls the application from the same directory as the service process.                                                                                                         |
| DIAG_PARAMETER     | (none)        | Diagnostic parameters. If the parameter has spaces, the parameter must be enclosed with quotation marks ("").                                                                                                                         |

### CPU Threshold Configuration

| resmon.ini            | Default value | Description                                                                                                                                                          |
|-----------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPU_LOAD_LIMIT        | 10            | Percentage CPU threshold at which either action is taken, or UPDATE_INTERVAL starts counting occurrences of reaching threshold.<br>The minimum is 1. Maximum is 100. |
| CPU_INTERVALS_ALLOWED | 10            | Number of intervals the CPU can be above the threshold before it triggers an action (used with UPDATE_INTERVAL to set a time limit).                                 |

| resmon.ini      | Default value | Description                                                                                                                                                                                                                                  |
|-----------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UPDATE_INTERVAL | 1             | Valid values: <ul style="list-style-type: none"> <li>• 0: Take action when CPU reaches its load limit.</li> <li>• 1: Take action when CPU reaches its load limit the number of times that are specified by CPU_INTERVALS_ALLOWED.</li> </ul> |

#### Memory Usage, Handle Count and Thread Count Thresholds Configuration

| resmon.withi                    | Default value | Description                                                                                                                         |
|---------------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------|
| MEM_USAGE_LIMIT                 | 150000        | Lower-level threshold in KB. An action is triggered if this limit is exceeded for more intervals than MEM_USAGE_INTERVALS_ALLOWED.  |
| MEM_USAGE_INTERVALS_ALLOWED     | 30            | Number of intervals allowed for the lower limit threshold before an action is triggered (used with UPDATE_INTERVAL for time limit). |
| MEM_USAGE_PEAK_LIMIT            | 200000        | Upper level threshold in KB. An action is triggered if this threshold is exceeded once.                                             |
| HANDLE_COUNT_LIMIT              | 500           | Lower-level threshold. An action is triggered if this limit is exceeded for more intervals than HANDLE_COUNT_INTERVALS_ALLOWED.     |
| HANDLE_COUNT_INTERVALS_ALL_Owed | 20            | Number of intervals allowed for the lower limit threshold before an action is triggered (used with UPDATE_INTERVAL for time limit). |
| HANDLE_COUNT_PEAK_LIMIT         | 1000          | Upper level threshold. An action is triggered if this threshold is exceeded once.                                                   |
| THREAD_COUNT_LIMIT              | 200           | Lower-level threshold. An action is triggered if this limit is exceeded for more intervals than THREAD_COUNT_INTERVALS_ALLOWED.     |
| THREAD_COUNT_INTERVALS_ALL_Owed | 20            | Number of intervals allowed for the lower limit threshold before an action is triggered (used with UPDATE_INTERVAL for time limit). |
| THREAD_COUNT_PEAK_LIMIT         | 300           | Upper level threshold. An action is triggered if this threshold is exceeded one time.                                               |

## Action Configuration

The actions that can be triggered are described under Core Dump Configuration and Diagnostic Configuration. The second and third actions are only initiated if they are triggered within the ACTION\_RESET\_INTERVAL of the previous action. If the ACTION\_RESET\_INTERVAL time has elapsed with no new triggers, then the next trigger starts a new cycle starts with the FIRST\_ACTION.

| resmon.ini             | Default value | Description                                                                                                                                                                                              |
|------------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FIRST_ACTION           | 1             | Valid values: <ul style="list-style-type: none"> <li>• 0: No action.</li> <li>• 1: Take action then restart the service.</li> <li>• 2: Take action then stop the service without restarting.</li> </ul>  |
| SECOND_ACTION          | 1             | Valid values: <ul style="list-style-type: none"> <li>• 0: No action.</li> <li>• 1: Take action then restart the service.</li> <li>• 2: Take action, then stop the service without restarting.</li> </ul> |
| THIRD_ACTION           | 2             | Valid values: <ul style="list-style-type: none"> <li>• 0: No action.</li> <li>• 1: Take action then restart the service.</li> <li>• 2: Take action, then stop the service without restarting.</li> </ul> |
| ACTION_RESET_INTERVALS | 60            | Number of seconds before resetting the action count. For example, if an action is triggered after more than 60 seconds since the previous action, FIRST_ACTION is applied.                               |

## Resource monitoring example

This example shows how the Guardium Agent Monitor (GAM) settings interact to provide meaningful information. This example tracks memory usage settings. However, the same pattern applies to other resources.

Let's say that you have the following settings:

- NAME=GUARDIUM\_STAP
- UPDATE\_INTERVAL=1
- MEM\_USAGE\_LIMIT=150000
- MEM\_USAGE\_INTERVALS\_ALLOWED=30
- MEM\_USAGE\_PEAK\_LIMIT=200000
- ACTION=1
- FULLDUMP=0
- DIAGACTION=1
- DIAGNAME=diag.bat
- FIRST\_ACTION=1
- ACTION\_RESET\_INTERVALS=60
- SECOND\_ACTION=2
- THIRD\_ACTION=2

GAM monitors memory usage of GUARDIUM\_STAP service (as specified in NAME) every second (UPDATE\_INTERVAL). If MEM\_USAGE-LIMIT exceeds 150 MB 30 consecutive times (MEM\_USAGE\_INTERVALS\_ALLOWED) or if MEM\_USAGE\_PEAK\_LIMIT exceeds 200 MB once, GAM takes the following actions:

- Generate a mini-dump (ACTION and FULLDUMP)
- Run `diag.bat` (DIAGACTION and DIAGNAME)

- Restart the service (FIRST\_ACTION).
- If the same symptoms occur within 60 seconds (ACTION\_RESET\_INTERVALS), GAM takes the same actions (SECOND\_ACTION).
- If the same symptoms occur again within 60 seconds, GAM generates a mini-dump, runs `diag.bat`, and stops the service without restarting (THIRD\_ACTION).

## Windows: Troubleshooting S-TAP problems

You can use the S-TAP Status monitor tab of the System View to begin investigating any problems. Sometimes you might need to use other tools, particularly if you are monitoring databases for which the inspection engines cannot be verified.

If an S-TAP is not connected to your Guardium® system

Check whether the IBM Security Guardium S-TAP service is running on the database server:

Check the IBM Security Guardium S-TAP service and see that it's running.

Make sure that sniffer is running on the server with the S-TAP service.

Check the communication between the sniffer and S-TAP.

For more information about possible errors, see [Table 2](#).

How to identify the S-TAP version?

- From the GUI, the S-TAP version number is displayed in `Manage > System View > S-TAP Status Monitor`
- Alternatively, you can display the S-TAP version number from the command line of the database server.

Run debug from the command line to quickly identify configuration issues

Turn on debug from the GIM GUI or the command line. See debug levels in [Debug parameters](#).

Verify the connection between the database server and the Guardium system

- Verify that you can ping the Guardium system at `sqlguard_ip` from the database server.
- If the ping is successful, verify that you can telnet to the following ports on the Guardium system: 9500/9501 for S-TAP on Protocol 7, or 9800/9801 for S-TAP on Protocol 8.

If there is a firewall between the database server and the Guardium system

Verify that the following ports are open for traffic between these two systems: TCP port 9500 or TLS port 9501 for encrypted connections for S-TAP on Protocol 7, or TCP port 9800 or TLS port 9801 for encrypted connections for S-TAP on Protocol 8.

Verify that the `sqlguard_ip` parameter is set to the correct guardium hostname or the IP for the Guardium system that you are connecting to.

1. Click `Manage > Activity Monitoring > S-TAP Control` to open S-TAP Control.
2. Locate the S-TAP Host for the IP address that corresponds to your database server.
3. Expand the Guardium Hosts subsection, and verify that the active Guardium Host is correctly configured.
4. If necessary, click Modify to update the Guardium Hosts.

Where is the debug file located?

If the debuglevel > 0, then the log from the previous S-TAP session (if it exists) is saved as: `%STAP_DIR%\Bin\StapBuffer\stap_%HOSTNAME%YY-MM-DD%HHMMDD%.old` and the new log is created as: `%STAP_DIR%\Bin\StapBuffer\stap_%HOSTNAME%YY-MM-DD%HHMMDD%.new`.

In addition to this, start-up logs containing just messages related to S-TAP start-up are always generated in `%STAP_DIR%\Logs: startup_%HOSTNAME%YY-MM-DD%HHMMDD%.old` startup\_%HOSTNAME%YY-MM-DD%HHMMDD%.new.

Severe spikes in traffic, and traffic getting dropped

This symptoms could be due to a buffer overflow. Check the debug log for a message indicating buffer overflow. Advanced users only: consider enabling the dynamic buffer feature. See `dynamic_buffer_increase` in [General parameters](#).

Verify that the S-TAP process is not repeatedly restarting

To verify the process, go to services and check the status of Guardium services.

Verify that S-TAP Approval is not turned on

If S-TAP Approval is turned on, any new S-TAP that connects to the Guardium system is refused.

1. Click `Manage > Activity Monitoring > S-TAP Certification` to open S-TAP Certification.
2. Look at the S-TAP Approval Needed checkbox. If this box is checked, new S-TAPs can connect to this Guardium system only after they are added to the list of approved S-TAPs.
3. If S-TAP Approval is turned on, access the Approved Tap Clients report to view a list of approved S-TAPs. If the S-TAP that you are investigating is not on this list, return to the S-TAP Certification page, enter the IP address of the S-TAP in the Client Host field, and click Add.

For more information, see [Allow \(approve\) S-TAP connection to Guardium \(S-TAP certification\)](#).

S-TAP verification issues

The verification process attempts to log in to your database's STAP client with an erroneous user ID and password to verify that this attempt is recognized and communicated to the Guardium system. Your S-TAP might be configured in a way that prevents the inspection engine message from reaching the Guardium system from which the request was made.

These configuration details include:

- Load balancing: if the S-TAP is configured to return responses to more than one Guardium system, the error message might be sent to a different Guardium system.
- Failover: If secondary Guardium systems are configured for the S-TAP, the error message might be sent to a secondary Guardium system if the primary Guardium system is too busy.
- `db_ignore_response`: if the S-TAP is configured to ignore all responses from the database, it does not send error messages to the Guardium system.
- Client IP/mask: if any mask is defined that is not 0.0.0.0, it might prevent the error message from being sent.
- Exclude IP/mask: if any mask is defined that is not 0.0.0.0, it might prevent the error message from being sent.

Related topics:

- [Windows: Monitoring S-TAP in the GUI](#)
- [Windows: Monitoring with the Guardium Agent Monitor](#)
- [Windows: Inspection engine verification](#)

## Windows: Scheduling S-TAP diagnostics

You can schedule S-TAP diagnostics by using the S-TAP Diagnostic Scheduler user interface.

### Before you begin

You must be logged in to the Guardium system that is the active host for the S-TAP®.

### Procedure

1. Browse to Manage > Activity Monitoring > S-TAP Diagnostic Scheduler.

You can see all the Windows S-TAP hosts that are listed under the S-TAP Hosts column that are managed by the Guardium system. This is the same list that is present on the S-TAP Control page.

2. Select one or more S-TAP hosts and click Add to schedule. The following options are available to run the diagnostics:

- Click Create Schedule to create a schedule to run the diagnostics and enter the details.
- Click Run Once to run the diagnostic immediately.

Important: After you run the diagnostics, click refresh to view the diagnostic results in the grid.

3. To remove the S-TAP hosts from the diagnostic schedule, select one or more S-TAP hosts from the S-TAP Hosts list and click Remove from schedule.

4. Optional: Click edit icon to edit the following S-TAP host details:

- Participate in scheduled diagnostics
- Level
- Duration

## Linux-UNIX: S-TAP user's guide

The Guardium S-TAP is a lightweight software agent installed on database servers and file servers. The S-TAP generally accounts for between 2% - 5% of CPU usage. In most installations, the impact is negligible with no noticeable impact on performance. The information collected by the S-TAPs is the basis of all Guardium traffic reports, alerts, visualizations, etc.

For data activity monitoring, the S-TAP monitors activity between the client and the database and forwards that information to the Guardium collector. The database traffic is logged into the collector based on criteria specified in the security policy. You can reduce the amount of traffic that is originally sent to the collector by ignoring trusted connections or ignoring traffic from specific IPs.

**MySQL limitations:** For MySQL, TCP is the only supported protocol. In addition, Windows S-TAP does not support MySQL encrypted traffic.

- [Linux-UNIX: S-TAP functionality](#)  
Familiarize yourself with these concepts before starting an S-TAP installation on a UNIX system.
- [Linux-UNIX: Installing, upgrading and uninstalling S-TAP agents](#)  
There are a few methods of installing, upgrading and uninstalling S-TAPs. Learn about each one and understand what works best for you.
- [Linux-UNIX: Configuring S-TAP](#)  
Learn to configure the S-TAP.
- [Linux-UNIX: S-TAP configuration per database type](#)  
This section provides detailed instructions or example for configuring monitoring on various databases.
- [Linux-UNIX: S-TAP operation and performance](#)

## Linux-UNIX: S-TAP functionality

Familiarize yourself with these concepts before starting an S-TAP installation on a UNIX system.

- [Linux-UNIX: S-TAP monitoring mechanisms support matrix](#)  
Select your S-TAP setup depending on the data you want to monitor or block. Use this table to identify the monitoring mechanisms (Exit libraries, K-TAP, A-TAP) that can perform the operations you require, per operating system and database.
- [Linux-UNIX: S-TAP monitoring mechanisms](#)  
The Guardium® UNIX S-TAP uses several different monitoring mechanisms to collect database traffic. During configuration, you can choose the method that best meets your requirements. All mechanisms filter the traffic to reduce network overhead and increase performance.
- [Linux-UNIX: S-TAP to collector encryption](#)  
S-TAP agents can be configured to communicate with collectors over the network in an encrypted (TLS) manner.
- [Linux-UNIX: UID chains](#)  
UID chain is a mechanism that allows S-TAP (by way of K-TAP) to track the chain of users that occurred before a database connection.
- [Linux-UNIX: Proxy firewall](#)  
Learn how to monitor traffic that originates from a proxy server.
- [Linux-UNIX: Using automation tools with the S-TAP and sample scripts](#)  
Guardium UNIX S-TAP has many script based interfaces to assist in the installation, configuration, and maintenance of the UNIX S-TAP agents. The following links provide you with the information necessary to create the automation scripts that work in your environment.

## Linux-UNIX: S-TAP monitoring mechanisms support matrix

Select your S-TAP setup depending on the data you want to monitor or block. Use this table to identify the monitoring mechanisms (Exit libraries, K-TAP, A-TAP) that can perform the operations you require, per operating system and database.

For example, you may want to track or perform one or more of the following:

- local traffic only
- local and network traffic
- shared memory
- encrypted data
- monitor and block
- monitor only

[Guardium support matrix](#) covers the most common platforms, database types, and protocols, supported by Guardium's monitoring mechanisms. The table presents general guidelines. There may be other combinations that are not presented here that are supported. Some of the supported setups presented here may be dependent on specific configurations. Contact Customer Support to verify the best setup for your specific needs. Empty cells indicate that the combination is not supported.

The exit libraries are preferred over all other monitoring mechanisms. If you cannot use an exit library, K-TAP is the next choice, then A-TAP, and finally PCAP.

## Linux-UNIX: S-TAP monitoring mechanisms

The Guardium® UNIX S-TAP uses several different monitoring mechanisms to collect database traffic. During configuration, you can choose the method that best meets your requirements. All mechanisms filter the traffic to reduce network overhead and increase performance.

You choose the mechanism during installation. All mechanisms filter the traffic so that only database-related traffic for specific sets of client and server IP addresses is collected. The mechanisms are presented here in order of preference: exit libraries, K-TAP, A-TAP, PCAP. See [Linux-UNIX: S-TAP monitoring mechanisms support matrix](#) and choose the mechanism that meets your needs.

### Exit libraries

The exit libraries are the preferred monitoring mechanism. They give the best performance, and can handle both local and network traffic, whether encrypted or not. They always capture DB\_USER. The only disadvantage is that exit libraries are supported only for Db2, Informix, and Teradata.

They require configuration on the database. If you upgrade the S-TAP version, then the exit library requires a restart, though you can restart whenever you choose. See [Linux-UNIX: Configuring Exit libraries](#).

### K-TAP

K-TAP is a kernel module that is installed into the operating system. It supports all protocols and connection methods (for example, TCP, TLI, SHM, Named Pipes). When enabled, it observes access to a database server by hooking into the mechanisms that are used to communicate between the database client and server. With Linux, the kernel frequently updates, and there are many kernel versions. The K-TAP version depends on the Linux version. See [Linux-UNIX: S-TAP compilation of K-TAP](#).

K-TAP is installed during S-TAP installation. If K-TAP fails to install, PCAP is installed instead. After it is installed, it can be enabled or disabled with a configuration file setting. If you do not load K-TAP during the S-TAP installation, and decide later that you want to use it, you need to reconfigure and restart the S-TAP.

### A-TAP

The A-TAP (application-level tap) sits in the application layer to support monitoring of encrypted database traffic, which cannot be done in the kernel by K-TAP. A-TAP monitors communication between internal components of the database server. It picks up unencrypted data in the application layer, and sends it to the K-TAP. K-TAP is a proxy to pass data to S-TAP, which then sends it to the Guardium collector.

With A-TAP, instead of capturing data from the kernel, where the data is still encrypted, Guardium captures data by loading a TAP library before executing the original database binary. The A-TAP libraries are a no-op (no interface). The libraries tap the database in application-mode, after the data is decrypted or before it is encrypted by the database. Hence there are no changes made to how the database would normally operate other than the encrypted traffic is now being captured by Guardium. This means that you do not need to update scripts and tools to call the Guardium code before executing the Oracle code.

A-TAP is included in every S-TAP but must be configured separately for each database instance to be monitored. See [Linux-UNIX: A-TAP management](#).

#### Restrictions:

- A-TAP is not supported in an environment where a 32-bit database is located on a 64-bit server.

#### When to use A-TAP?

A-TAP is required when DBMS encryption in motion is used, but there may be other internal database implementation details such as shared memory that require it.

Informix and Db2 on Linux integrate with Guardium more closely using an exit and thus are the recommended method for shared memory support when applicable.

### PCAP

PCAP is a packet-capturing mechanism that listens to network traffic from and to a database server. In a UNIX environment, since the K-TAP captures all network traffic, PCAP is rarely used. PCAP is used to capture local TCP/IP traffic on the device.

#### Restriction:

- PCAP only works on ports (no shared memory, and so on).

The PCAP uses the client IP/mask values for all local inspection engines to determine what to monitor and report. A PCAP that is installed with an S-TAP with multiple inspection engines that have different client IP/mask values, captures traffic from all clients that are defined in all inspection engines. The PCAP might be processing and sending more information to the Guardium system than you intend.

## Linux-UNIX: S-TAP to collector encryption

S-TAP agents can be configured to communicate with collectors over the network in an encrypted (TLS) manner.

Guardium recommends encrypting network traffic between the S-TAP and the collector whenever possible, only in cases where the performance is a higher priority than security should this be disabled. There is a small impact on performance when enabling encryption. The default S-TAP configuration is no encryption, to avoid any performance impact.

Before you determine the best choice for your environment, consider the following factors:

- Configuring the S-TAP with TLS requires extra time for encryption that might affect performance on the database server where the S-TAP agent is installed. The appliance (collector) also requires time to decrypt this traffic.
- If applications and database users are communicating with the database in an unencrypted manner, configuring the S-TAP agent to communicate over the network with encryption may not make your network safer.

In general, it makes sense to encrypt S-TAP traffic if the data that is sent to an appliance on a different network is encrypted, or if the database traffic that is monitored is network encrypted.

Encryption is enabled during the inspection engine configuration, and can be modified at any time.

## Linux-UNIX: UID chains

UID chain is a mechanism that allows S-TAP (by way of K-TAP) to track the chain of users that occurred before a database connection.

You can change usernames several times before you connect to the database. For example, you can run the following commands: **ssh informix@barbet**, then **su - db2inst1**, then **su -**, then **su - oracle9**, and end with **sqlplus scott/tiger@onora1**. With UID Chains, Guardium® can trace this process back to the process that called it, and back to the original (offending) user.

The UID chain values vary by OS platform. For example, under AIX the string IBM might appear as a prefix. For MongoDB, you can use a UID chain to determine the DB\_USER for reports, as MongoDB does not include OS\_USER in the login packet.

Enabling UID chains should not affect performance.

See the [Guardium support matrix](#) for a full list of operating systems and databases that support UID chains.

## Limitations

- For Solaris Zones, user IDs might be reported instead of usernames.
- The SSH client's IP address and port are added to the UID chain.
- PostgreSQL on Solaris 11 with zones is not supported, due to zone configuration not allowing access from primary to subordinate zones in some directories.
- Solaris Zones and AIX® WPAR - set the db2bp\_path in the guard\_tap.ini file to the full path of the db2bp executable file (the full path of the relevant db2bp as seen from the global zone/wpar).
- UID Chains are not reported for Inter-process Communication (IPC) on Solaris 8/9.
- UID chains are not detected for Hadoop databases.
- UID chain does not support local TCP on Linux for Db2. In addition, Db2 exit requires a specific version of the database to support UID chains.
- When running as a non-root user, UID chain does not work for Db2 Shared Memory (SHM) with S-TAP.
- Guardium does not log UID chain for network traffic.
- Guardium might not log UID chain for very short sessions since Guardium relies on the process ID of the application to determine the UID chain. If the process that starts the session exits before S-TAP can examine it, UID chain does not work.
- UID is not captured for Cassandra Datastax when Audit logging is used.
- UID is not captured for Cassandra Apache when Audit logging is used.
- UID chain is supported in these scenarios that require A-TAP for intercepting the traffic:
  - Sybase SSL traffic when the min and max port are set in the executor.
  - Mongo and Postgres SSL traffic.
  - Teradata encrypted traffic.

All other scenarios that require A-TAP are not supported.

## Configuring UID chain

You can control UID configuration with the following parameters,

- **hunter\_trace** - Enable this guard\_tap.ini parameter to log UID chain for all database connections.
- **uid\_chain\_sshd\_ip** - Enables adding an SSH client IP:port to the UID chain when SSH is identified as one of the processes in the chain.

The UID chains are logged in the collectors,

- **UID\_CHAIN** - The full chain of users, for example,  

```
(1,root,init [5])>(3746,root,/usr/sbin/sshd -o PidFile=/var/run/sshd.init.pid)>
(6948,root,sshd: root@pts/2)>(6950,root,-bash)>(7481,root,su - informix)>(7482,informix,-bash)>
(7522,informix,su - db2inst1)>(7523,db2inst1,-bash)>(7941,db2inst1,su - oracle12)>
(7942,oracle12,-bash)>(7982,oracle12,sqlplus)
```
- **UID\_CHAIN\_COMPRESSED** - The UID chain, excluding the first user and the last user, in this example, *informix, db2inst1*.

## UID chains in reports

To view UID chains in reports, use the UID Chain and UID Chain Compressed attributes in the Session entity.

Note: When you call the UID Chain or UID Chain Compressed attributes in a report, you might see a delay of up to 3 minutes in the UID Chain response. UID chains can be logged to Syslog with %%compressed\_uid\_chain or %%uid\_chain alert messages.

## Purging of UID chain records

UID chain records that are older than 2 hours are purged when the regular inference process runs. (Inference goes over all the records and consolidates them.) Records that are older than 24 hours are purged on a nightly basis.

## Related reference

- [Linux-UNIX: General parameters](#)

## Linux-UNIX: Proxy firewall

Learn how to monitor traffic that originates from a proxy server.

While S-TAP is normally deployed on a database server, a K-TAP based firewall can be deployed to a proxy server. By utilizing S-GATE, you can monitor traffic that originates from the proxy server. See [Linux-UNIX: Application server parameters](#) and S-GATE Actions (Blocking Actions) in the Policies help topic for more information on setting appserver parameters and using S-GATE within Policies.

## Linux-UNIX: Using automation tools with the S-TAP and sample scripts

Guardium UNIX S-TAP has many script based interfaces to assist in the installation, configuration, and maintenance of the UNIX S-TAP agents. The following links provide you with the information necessary to create the automation scripts that work in your environment.

|                                                |                                                                                                             |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| A-TAP management                               | <a href="#">Linux-UNIX: A-TAP management</a>                                                                |
| Using guardctl for A-TAP                       | <a href="#">Linux-UNIX: guardctl utility commands for A-TAP</a>                                             |
| Return codes for guardctl                      | <a href="#">Linux-UNIX: guardctl return codes</a>                                                           |
| Installing S-TAP with GIM                      | <a href="#">Linux-UNIX: Installing the S-TAP client with GIM Setup by Client</a>                            |
| Modifying S-TAP configuration with GIM         | <a href="#">Set up by Client</a> and <a href="#">Linux-UNIX: Editing the S-TAP configuration parameters</a> |
| Uninstalling S-TAP with GIM                    | <a href="#">Linux-UNIX: Uninstalling S-TAP agent with GIM Setup by Client</a>                               |
| Upgrading S-TAP with GIM                       | <a href="#">Linux-UNIX: Upgrading an S-TAP agent with GIM Setup by Client</a>                               |
| GIM S-TAP parameters                           | <a href="#">Linux-UNIX: S-TAP GIM installation parameters</a>                                               |
| Using guard-config-update                      | <a href="#">Linux-UNIX: Using guard-config-update to start, restart, and stop S-TAP, and view status</a>    |
| Configuring S-TAP with guard-config-update     | <a href="#">Linux-UNIX: Configure S-TAP with guard-config-update</a>                                        |
| Installing the S-TAP using the shell installer | <a href="#">Linux-UNIX: Installing the S-TAP client by using the shell installer</a>                        |
| Uninstalling S-TAP with the shell installer    | <a href="#">Linux-UNIX: Uninstalling S-TAP agents using the shell installer</a>                             |
| Upgrading S-TAP with the shell installer       | <a href="#">Linux-UNIX: Upgrading the S-TAP agent using the shell installer</a>                             |
| Install script parameter for S-TAP             | <a href="#">Linux-UNIX: S-TAP install script parameters</a>                                                 |

The following Ansible playbooks can be used as examples for install, activation of A-TAP, deactivation of A-TAP, and uninstall.

## Install S-TAP sample

```

- hosts: all
 vars:
 guardium_appliance: my-collector.example.com
 installer_dir: ./

 installer: guard-stap-11.2.0.0_r108838_v11_2_1-rhel-8-linux-x86_64.sh
 destination: /var/tmp
 install_dir: /usr/local
 tasks:
 - name: Check for previous installation
 block:
 - name: Look for KTAP
 shell: lsmod | grep ktap
 register: lsmod_out
 ignore_errors: yes
 - name: Look for existing installation directory
 stat:
 path: "{{ install_dir }}/{{ guardium }}"
 register: guardium_dir
 - name: Installation
 block:
 - name: Copy shell installer
 copy:
 src: "{{installer_dir}}/{{ installer }}"
 dest: "{{ destination }}"
 owner: root
 group: root
 mode: 0755
 become: yes
 - name: Do shell installation
 block:
 - name: Run shell installer
 shell: "{{ destination }}/{{ installer }} --ni -k --dir {{ install_dir }} --tapip {{ ansible_hostname }} --
sqlguardip {{ guardium_appliance }} --ktap_allow_module_combos"
 register: installer_output
 become: yes
 - debug:
 msg: "{{ installer_output.stderr }}"
 - debug:
 msg: "{{ installer_output.stdout }}"
 when: guardium_dir.stat.exists == false and lsmod_out.stdout == ""
 - name: Check KTAP
 shell: lsmod | grep ktap
```

```

 register: lsmod_out
 - debug:
 msg: "{{ lsmod_out.stdout }}"

```

## Uninstall S-TAP sample

---

```

- hosts: all
 vars:
 install_dir: /usr/local
 tasks:
 - name: Check if STAP is installed
 stat:
 path: "{{ install_dir }}/guardium/guard_stap/uninstall"
 register: uninstall_script
 - name: Do uninstall
 block:
 - name: Run uninstall
 shell: "{{ install_dir }}/guardium/guard_stap/uninstall"
 register: uninstall_output
 become: yes
 - debug:
 msg: "{{ uninstall_output.stderr }}"
 - debug:
 msg: "{{ uninstall_output.stdout }}"
 when: uninstall_script.stat.exists == true
 - name: Check if KTAP is loaded
 shell: lsmod | grep ktap
 register: lsmod_ktap
 ignore_errors: yes
 - name: Reboot
 reboot:
 reboot_timeout: 3600
 become: yes
 when: lsmod_ktap.rc == 0
 - name: Verify no KTAP
 shell: lsmod | grep ktap
 register: result
 failed_when:
 - result.rc == 0

```

## Activate A-TAP sample

---

```

- hosts: all
 vars:
 install_dir: /usr/local
 db_user: oracle11
 db_base: /opt/oracle11
 db_home: "{{ db_base }}/product/11.1.0/db_1"
 db_version: 11
 db_type: oracle
 db_instance: oracle11
 restart_db: false
 stop_db: false
 tasks:
 - name: Check if ATAP is already active
 shell: "{{ install_dir }}/guardium/guard_stap/guardctl list-active | grep \"root/{{ db_instance }}\""
 ignore_errors: yes
 register: atap_grep
 - name: ATAP is not already active
 block:
 - name: Verify DB is in IEs
 block:
 - name: Grep for DB_HOME in IEs
 shell: "{{ install_dir }}/guardium/guard_stap/guard-config-update --show-ies | grep \"{{ db_install_dir }}*={{ db_base }}\""
 ignore_errors: yes
 register: ie_grep
 - name: Run discovery and re-check IEs
 block:
 - name: Check if DB is running
 shell: ps -ef | grep -v grep | grep oracle11 | grep tnslnsr
 register: oracle_ps
 ignore_errors: yes
 - name: DB is not running, needs to be started
 block:
 - name: Run startup command
 shell: "su - {{ db_user }} -c \"{{ db_base }}/START.sh\""
 ignore_errors: yes
 register: cmd_output
 become: yes
 - debug:
 msg: "{{ cmd_output.stdout }}"
 - debug:
 msg: "{{ cmd_output.stderr }}"
 - set_fact:
 stop_db: true
 when: oracle_ps.rc != 0
 - name: Run discovery
 shell: "{{ install_dir }}/guardium/guard_stap/guard_discovery {{ install_dir }}/guardium/guard_stap/guard_tap.ini
--update_tap"
 become: yes

```

```

 - name: Grep for DB HOME in IEs
 shell: "{{ install_dir }}/guardium/guard_stap/guard-config-update --show-ies | grep \"db_install_dir[]*=[]*{{ db_base }}\""
 when: ie_grep.rc != 0
 - name: Leave DB down if it wasn't started
 block:
 - name: Run shutdown command
 shell: "su - {{ db_user }} -c \"{{ db_base }}/STOP.sh\""
 ignore_errors: yes
 register: cmd_output
 become: yes
 - debug:
 msg: "{{ cmd_output.stdout }}"
 - debug:
 msg: "{{ cmd_output.stderr }}"
 when: stop_db == true
 - name: Check if DB is running
 shell: ps -ef | grep -v grep | grep oracle11 | grep tnslsnr
 register: oracle_ps
 ignore_errors: yes
 - name: Shut down database
 block:
 - name: Run shutdown command
 shell: "su - {{ db_user }} -c \"{{ db_base }}/STOP.sh\""
 ignore_errors: yes
 register: cmd_output
 become: yes
 - debug:
 msg: "{{ cmd_output.stdout }}"
 - debug:
 msg: "{{ cmd_output.stderr }}"
 - set_fact:
 restart_db: true
 when: oracle_ps.rc == 0
 - name: Activate ATAP
 shell: "{{ install_dir }}/guardium/guard_stap/guardctl --db-user={{ db_user }} --db-type={{ db_type }} --db-instance={{ db_instance }} --db-base={{ db_base }} --db-home={{ db_home }} --db-version={{ db_version }} activate"
 become: yes
 - name: Restart DB
 block:
 - name: Run startup command
 shell: "su - {{ db_user }} -c \"{{ db_base }}/START.sh\""
 register: cmd_output
 become: yes
 - debug:
 msg: "{{ cmd_output.stdout }}"
 - debug:
 msg: "{{ cmd_output.stderr }}"
 when: restart_db == true
when: atap_grep.rc != 0

```

## Deactivate A-TAP sample

---

```

hosts: all
vars:
 install_dir: /usr/local
 db_user: oracle11
 db_base: /opt/oracle11
 db_instance: oracle11
 restart_db: false
 stop_db: false
tasks:
 - name: Check if ATAP is active
 shell: "{{ install_dir }}/guardium/guard_stap/guardctl list-active | grep \"root/{{ db_instance }}\""
 ignore_errors: yes
 register: atap_grep
 - name: ATAP is active
 block:
 - name: Check if DB is running
 shell: ps -ef | grep -v grep | grep oracle11 | grep tnslsnr
 register: oracle_ps
 ignore_errors: yes
 - name: Shut down database if is up
 block:
 - name: Run shutdown command
 shell: "su - {{ db_user }} -c \"{{ db_base }}/STOP.sh\""
 ignore_errors: yes
 register: cmd_output
 become: yes
 - debug:
 msg: "{{ cmd_output.stdout }}"
 - debug:
 msg: "{{ cmd_output.stderr }}"
 - set_fact:
 restart_db: true
 when: oracle_ps.rc == 0
 - name: Deactivate ATAP
 shell: "{{ install_dir }}/guardium/guard_stap/guardctl --db-instance={{ db_instance }} deactivate"
 become: yes
 - name: Restart DB
 block:
 - name: Run startup command
 shell: "su - {{ db_user }} -c \"{{ db_base }}/START.sh\""

```

```

register: cmd_output
become: yes
- debug:
 msg: "{{ cmd_output.stdout }}"
- debug:
 msg: "{{ cmd_output.stderr }}"
when: restart_db == true
when: atap_grep.rc == 0

```

## Linux-UNIX: Installing, upgrading and uninstalling S-TAP agents

There are a few methods of installing, upgrading and uninstalling S-TAPs. Learn about each one and understand what works best for you.

- [Linux-UNIX: Install S-TAP agents installation flow](#)

Verify prerequisites, then install an S-TAP on Linux, Solaris, AIX and HP-UX servers using the Deploy Monitoring Agents tool, Guardium Installation Manager (GIM), the RPM, or the shell installer.

- [Linux-UNIX: S-TAP installation prerequisites](#)

Verify all prerequisites before starting your S-TAP installation.

- [Linux-UNIX: Before you start installing S-TAP](#)

Read these notes before you start to install an S-TAP.

- [Linux-UNIX: Use GIM to install, upgrade, uninstall the S-TAP](#)

- [Linux-UNIX: Use RPM to install, upgrade, uninstall the S-TAP](#)

You can manage your S-TAP agent with .rpm on RHEL and for SUSE Linux databases.

- [Linux-UNIX: Use shell installer to install, upgrade, uninstall the S-TAP](#)

- [Linux-UNIX: Use native installers to install, upgrade, uninstall the S-TAP](#)

The native installer provides a shell for the shell installer. The only advantage is that it ensures that S-TAP is registered in the operating system asset repository. This registration is not required by Guardium® for the installation of the S-TAP, but it might be a requirement at your company. Use the native installer only when necessary.

- [Linux-UNIX: S-TAP upgrade workflows per monitoring mechanism](#)

The S-TAP upgrade workflow depends on your monitoring mechanism: K-TAP, exit library, A-TAP. Use these workflows together with the specific upgrade procedure.

- [Linux-UNIX: Working with K-TAP](#)

K-TAP is a kernel module that is installed into the database server operating system during S-TAP installation. After it is installed, it can be enabled or disabled with a configuration file setting. When enabled, it observes access to a database server by hooking the mechanisms used to communicate between the database client and the server. With K-TAP you do not need to change how database clients connect to the server.

- [Linux-UNIX: Special environments configuration](#)

Use these procedures for as relevant for systems with Zones, RAC, WPAR, clusters.

- [Linux-UNIX: What to restart or reboot on the database server after installing or updating S-TAP](#)

This topic details what needs to be rebooted or restarted after you install or upgrade your UNIX or Linux S-TAP. Restart and reboot requirements are the same for GIM and non-GIM implementations.

- [Linux-UNIX: Managing a GIM-, RPM-, and shell-installed S-TAP during a database upgrade](#)

Only the A-TAP needs handling when you upgrade a database with a GIM, RPM, or shell-installed UNIX S-TAP. If a system is running multiple databases, the S-TAP can continue to run and monitor all other databases not being upgraded.

- [Linux-UNIX: Managing GIM clients during a major upgrade of the database server operating system](#)

When you upgrade the operating system on your database server, use the GIM client to automatically upgrade itself and the GIM bundles (for example, GIM, S-TAP, CAS) installed on the Linux-UNIX database. However, most operating systems do not support a major upgrade, for example from RHEL7 to RHEL8.

- [Linux-UNIX: Managing an RPM- or shell-installed S-TAP during a major upgrade of the database server operating system](#)

When you upgrade the operating system on your database server, you need to uninstall the S-TAP, and install a new version. However, most operating systems do not support a major upgrade, for example, from RHEL7 to RHEL8.

- [Linux-UNIX: Managing a GIM-, RPM-, or shell-installed S-TAP during a minor or kernel upgrade of the database server operating system](#)

A minor database operating system upgrade can include a new operating system kernel. Use this task for both a minor upgrade or a kernel upgrade.

## Linux-UNIX: Install S-TAP agents installation flow

Verify prerequisites, then install an S-TAP on Linux, Solaris, AIX and HP-UX servers using the Deploy Monitoring Agents tool, Guardium Installation Manager (GIM), the RPM, or the shell installer.

Depending on your license key, you can use the same S-TAP agent for both file server and database activity monitoring. FAM does not require any specific S-TAP configuration.

This flow describes installing S-TAP on a single database reporting to one collector. See the related topics for additional information on S-TAP in clusters and zones.

1. Plan the installation, review these topics:

- [Linux-UNIX: S-TAP monitoring mechanisms support matrix](#)
- [Linux-UNIX: S-TAP monitoring mechanisms](#)
- [Linux-UNIX: S-TAP to collector encryption](#)
- [Enterprise Load Balancing](#)

2. Verify prerequisites.

- [Linux-UNIX: Database version and directory requirements](#)
- The database has sufficient disk space available ([Linux-UNIX: Disk space requirements for S-TAP](#)).
- The ports that are required for communication between the collector and the S-TAP are open ([Linux-UNIX: Port requirements for S-TAP](#)).
- Identify required IP addresses and check database connectivity ([Linux-UNIX: System details and checks](#)).
- If you are installing with GIM, the GIM client must be installed on the target database server. See [Installing the GIM client on a UNIX server](#).

3. Install S-TAP by one of

- [Deploy monitoring agents](#)
- [Linux-UNIX: Installing the S-TAP client with GIM Setup by Client](#)
- [Linux-UNIX: Installing the S-TAP agent with RPM](#)

- [Linux-UNIX: Installing the S-TAP client by using the shell installer](#)

During S-TAP installation, if auto-discovery is enabled, it auto-discovers databases and creates inspection engines for the discovered databases. The auto-discovery process runs once at the time of S-TAP installation and does not automatically repeat. You can modify the configuration after the installation is complete.

4. Configure any of the optional components if required by your system.

- [Linux-UNIX: Kerberos-authenticated database traffic](#)
- [Linux-UNIX: Solaris Zones configuration](#)
- [Linux-UNIX: Oracle RAC S-TAP configuration](#)
- [Linux-UNIX: Configure S-TAP for Db2 WPAR](#)
- [Linux-UNIX: Configure S-TAP for SELinux](#)
- [Linux-UNIX: Activating and deactivating A-TAP on all nodes of a Db2 Cluster](#)
- [Linux-UNIX: Configure delayed cluster disk mounting](#)

5. Reboot or restart if required ([Linux-UNIX: What to restart or reboot on the database server after installing or updating S-TAP](#)).

6. Complete the S-TAP configuration.

- [Linux-UNIX: Configuring S-TAP in the S-TAP Control page](#)
- Advanced users only: [Linux-UNIX: Editing the S-TAP configuration parameters](#)

7. If required, configure [Enterprise Load Balancing](#).

## Linux-UNIX: S-TAP installation prerequisites

Verify all prerequisites before starting your S-TAP installation.

- [Linux-UNIX: Database version and directory requirements](#)

Review these database releases, patch level components, and directories, before you install an S-TAP or any associated agent.

- [Linux-UNIX: Disk space requirements for S-TAP](#)

Review these disk space requirements before you install an S-TAP or any associated agent.

- [Linux-UNIX: Port requirements for S-TAP](#)

If a firewall is located between the Guardium® system and an S-TAP agent, verify that the ports that are used for connections between those components are open.

- [Linux-UNIX: System details and checks](#)

Verify these prerequisites, including system details; and that your database is communicating with Guardium .

## Linux-UNIX: Database version and directory requirements

Review these database releases, patch level components, and directories, before you install an S-TAP or any associated agent.

Table 1. Linux, Solaris, AIX and HP-UX database versions requirements

| DB Type                    | Version                                                                                                                                                                             |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Linux                      | make version 3.81 or later. To view your version of the make utility, run the command: <code>make -v</code>                                                                         |
| Oracle ASO, HP-UX<br>11.11 | LD_PRELOAD must be installed. It is installed by patch PHSS_28436 or later.                                                                                                         |
| TLS                        | For S-TAP on a server, either /dev/random or /dev/urandom must be present on the server. See the TLS port requirements in <a href="#">Linux-UNIX: Port requirements for S-TAP</a> . |

Note: A root user that installs GIM or S-TAP needs permissions to create and delete users and groups.

Table 2. Required directories per platform

| Requirement Type                               | Linux                                       | Solaris                                     | AIX                                         | HP-UX                                       |
|------------------------------------------------|---------------------------------------------|---------------------------------------------|---------------------------------------------|---------------------------------------------|
| Installation folder does not exist or is empty | /usr/local/guardium/guard_stap              | /usr/local/guardium/guard_stap              | /usr/local/guardium/guard_stap              | /usr/local/guardium/guard_stap              |
| File exists                                    | /bin/sh                                     | /bin/sh                                     | /bin/sh                                     | /bin/sh                                     |
| File exists                                    | /bin/sed or /usr/bin/sed                    | /bin/sed or /usr/bin/sed                    | /bin/sed or /usr/bin/sed                    | /bin/sed or /usr/bin/sed                    |
| File exists                                    | tar, awk, grep, tr                          |
| File exists                                    | dd and /dev/zero                            | dd and /dev/zero                            | dd and /dev/zero                            | prealloc                                    |
| File exists                                    | uuencode in /usr/bin or /tmp or perl exists | uuencode in /usr/bin or /tmp or perl exists | uuencode in /usr/bin or /tmp or perl exists | uuencode in /usr/bin or /tmp or perl exists |

## Linux-UNIX: Disk space requirements for S-TAP

Review these disk space requirements before you install an S-TAP or any associated agent.

Table 1. Linux, Solaris, AIX, and HP-UX: S-TAP disk space requirements

| Item | Disk Space |
|------|------------|
|------|------------|

| Item                | Disk Space                                                                                                                                                                                                                                                                                                                     |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| S-TAP program files | GIM Installation <ul style="list-style-type: none"> <li>• AIX: 400 MB</li> <li>• HP-UX: 500 MB</li> <li>• Linux: 450 MB</li> <li>• Solaris: 400 MB</li> </ul><br>non-GIM Install: <ul style="list-style-type: none"> <li>• AIX: 300 MB</li> <li>• HP-UX: 400 MB</li> <li>• Linux: 350 MB</li> <li>• Solaris: 300 MB</li> </ul> |
| FAM program files   | 600 MB minimum                                                                                                                                                                                                                                                                                                                 |
| Buffer file         | By default, the S-TAP uses anonymous memory to stage data for transmission to the Guardium system. If you configure the S-TAP to use a buffer file, the size defaults to 50 MB. The size is controlled by the <code>buffer_file_size</code> parameter in the <code>guard_tap.ini</code> file.                                  |

## Linux-UNIX: Port requirements for S-TAP

If a firewall is located between the Guardium® system and an S-TAP agent, verify that the ports that are used for connections between those components are open.

Use your firewall management utility to check, and open as relevant, the ports listed.

Table 1. Port Requirements for Linux, Solaris, AIX and HP-UX servers

| Port  | Protocol | Guardium system connection to ... |
|-------|----------|-----------------------------------|
| 16016 | TCP      | Clear S-TAP                       |
| 16018 | TLS      | Encrypted S-TAP                   |
| 16020 | TCP      | Regular pooled connections        |
| 16021 | TLS      | TLS pooled connections            |
| 16022 | TCP      | Feed protocol                     |
| 16023 | TLS      | Encrypted S-TAP TLS               |

## Linux-UNIX: System details and checks

Verify these prerequisites, including system details; and that your database is communicating with Guardium .

- Obtain the IP address of the database server on which you are installing S-TAP. If virtual IPs are used, note those as well (you will need to configure those later, when completing the configuration).
- If installing on the central manager, identify the IP address of the collector that will control this S-TAP, and to which this S-TAP will report.
- If installing on a server with secure boot enabled, enroll the Guardium S-TAP key on the database server before installing S-TAP. For more information, see [Linux-UNIX: Enrolling a K-TAP signing key](#).
- If installing a locally built (custom) K-TAP with secure boot on, use the `kernelModuleSigning.sh` utility to sign the K-TAP. For more information, see [Linux-UNIX: Signing and enrolling a locally built K-TAP](#).
- Verify connectivity between the database server and the collector. On the database, enter `nmap -p <port> <ip_address>`. For example, to check that port 16018 (the port Guardium uses for TLS) is reachable at IP address 192.168.3.104, enter the command `nmap -p 16018 192.168.3.104`

Typical output looks like:

```
Starting nmap V. 3.00 Interesting ports on g4.guardium.com (192.168.3.104): Port State Service 16018/tcp open unknown
```

## Linux-UNIX: Before you start installing S-TAP

Read these notes before you start to install an S-TAP.

When you install an S-TAP agent, the installation program checks whether the `guardium` group exists. If the group does not exist, the installation program creates it. If you use certain components or features, such as A-TAP or Db2 Exit, you must add users to this group to ensure proper functioning. These requirements are described in the relevant sections.

The installation process creates log files for the entire S-TAP package (S-TAP, K-TAP, A-TAP, PCAP, and Discovery). The log files are good for troubleshooting failed installations. Locations include `/var/tmp`, `/tmp`, and `/var/log`.

The installation process updates `inittab`, `upstart`, and `rc` scripts.

S-TAP installs into `/usr/local/guardium`.

When you define the [Linux-UNIX: S-TAP install script parameters](#), Guardium® suggests that you keep the default settings (`--userinst` and `--root`). These choices install the files with the `guardium` user as the owner, but keeps the appropriate privileges when the S-TAP runs.

When you define the installation script parameters, you can specify the installer user as either *root* (–rootinst) or the guardium user (–userinst). When the installer populates the files, it can populate them so they are owned by either the root user or by the guardium user. When the S-TAP runs, it always starts as the user *root*, but if you specify –user, then the S-TAP drops privileges to the guardium user level after it starts running.

Note: You cannot specify –rootinst with –user because the privileges don't line up. In this case, the installer returns an error and exits. Additionally, if the files are owned by *root*, you cannot run as *user*.

If you choose to run the S-TAP as the guardium *user* (and not *root*), you might encounter some issues and limitations. Running S-TAP as the guardium user can cause some databases or protocols to stop working because of permission levels. Verify that the database path or exec file has permission that allows the user guardium to read. Depending on your environment, limitations can include,

- Discovery has limited functionality.
- Database on AIX® WPAR and Solaris Zones might not work, check the permission to access the installation path or exec file.
- For Oracle BEQ, restart S-TAP after you start or restart the database.
- For Informix® shared memory, restart S-TAP after you start or restart the database.
- For Db2 shared memory,
  - When ktap\_fast\_shmem is set to 0, if **shmctl** fails because of permission issues, then in most cases, change the S-TAP to run as *root*.
  - When ktap\_fast\_shmem is set to 1, if shared memory segment has *read permission by group*, then make sure that the Db2 instance is added to user (Guardium) group. On each server, only one Db2 configuration is supported.
  - If shared memory segment has *read permission by Db2 user only*, then S-TAP must run as *root*. (Open a Db2 shared memory session, run the command **ipcs -ma**, and check MODE on the output.)

## Linux-UNIX: Use GIM to install, upgrade, uninstall the S-TAP

### • [Linux-UNIX: Installing the S-TAP client with GIM Setup by Client](#)

Use the Guardium® Installation Manager Setup by Client to install the S-TAP agent either from a stand-alone Guardium appliance, or from the Central manager to schedule installation on one or more databases.

### • [Linux-UNIX: S-TAP GIM installation parameters](#)

Understand the parameters (each with a short description) that are typically used in your GIM S-TAP agent installation.

### • [Linux-UNIX: Upgrading an S-TAP agent with GIM Setup by Client](#)

Use the GIM tool to upgrade your S-TAP agent.

### • [Linux-UNIX: Uninstalling S-TAP agent with GIM Setup by Client](#)

Learn how to uninstall the S-TAP agent and the GIM bundle from the database server. If S-TAP was installed with GIM it's highly recommend to uninstall with GIM. Otherwise you would need to manually remove the S-TAP folder from the GIM directory on the DB server.

## Linux-UNIX: Installing the S-TAP client with GIM Setup by Client

Use the Guardium® Installation Manager Setup by Client to install the S-TAP agent either from a stand-alone Guardium appliance, or from the Central manager to schedule installation on one or more databases.

### Before you begin

- Verify all [Linux-UNIX: S-TAP installation prerequisites](#).
- Obtain the correct S-TAP installer script, from either [Fix Central](#), or your Guardium representative. The script name identifies the database server operating system.

### About this task

After the installation, you can manage all parameters and monitor processes that were installed under its control. If you install by using one of the other installation methods, fewer agent parameters can be modified using GIM.

### Procedure

1. Verify that the GIM client is installed on the database server. See [Installing the GIM client on a UNIX server](#).
2. Upload the relevant S-TAP module to the Guardium Installation Manager appliance.
  - a. Go to **Manage > Module Installation > Upload Modules**.
  - b. Click **Choose File** and select the S-TAP module that you want to install.
  - c. Click **Upload** to upload the module to the appliance.The module appears in the Import Uploaded Modules table.
  - d. In the Import Uploaded Modules table, click the check box next to the S-TAP module you want to install.The module imports and becomes available for installation. The Upload Modules page resets and the Import Uploaded Modules table is now empty.
3. Navigate to **Manage > Module Installation > Set up by Client**.
4. In the Choose clients section, select the database servers where you want to install the S-TAP module. Select individual clients using check boxes in the table, or use the **Select client group** menu to select a group of clients. Click **Next** to continue.

Attention:

  - To create a client group, click  to open the Create client group dialog. Click **Add Clients** to open the Existing Clients window, select the clients, and click **OK**.
  - To import clients from a CSV file. Click **Import from CSV**, and selecting your CSV file. Modify the field delimiter if relevant. Click **Load** to create a group of type Client Hostname, with Application type of Public. This group can be accessed and managed from the Group Builder.
  - After you modify the client list, click  to update the display.
  - Use **Reset Connection** to remove GIM client information from the Guardium system before reregistering the client. After clicking **Reset Connection**, it might take a few minutes before the status of the GIM client process is reflected.

- Select a client and click View Installed Modules. The View Installed Modules window shows all the modules that are installed on this client (including S-TAP), their versions, and if any module is in pending state for all the selected clients. (The module COMMON, if it appears, can be ignored.)
  - When you create or update a group and edit the Client Name of GIM clients, the host name and address must reflect a valid value for a GIM client that is connected to the Guardium system. If an invalid host name is specified, the edited client does not appear as a member of the group. Adding clients by IP address is not supported.
5. In the Choose bundle section, use the Select a bundle menu to identify the software you want to install.  
After selecting a software bundle, the Selected bundle action column indicates Install, the action that will be performed for each client:
- Tip:
- You can filter the clients, for example, by name, module, Selected bundle actions, and client OS. The resulting selection is persistent; **the action is applied only to the filtered list of clients**. You can see that the number of clients in the Choose Clients section is greater than the number in Configure Clients section.
  - Clear the Show only latest versions checkbox to view and work with earlier versions of a bundle.
  - Clear the Show only bundles checkbox to identify individual modules within a bundle.
  - Select the Show only compatible clients checkbox to hide clients that are not compatible with the selected bundle.
- Attention:
- By default, the Select a bundle menu shows only the latest uploaded bundle version regardless of platform or compatibility with selected clients. To install a different bundle version for a specific platform or client, clear the Show only latest versions check box and select the required bundle.
  - If you upload and import new bundles while using the Set up by Client tool, refresh the browser to see the new bundles.
  - If you already have a bundle scheduled for installation, installing a new bundle removes the existing schedule.
- Click Next to continue.
6. In the Choose parameters section, specify values for required and optional parameters. Use the or to add or remove optional parameters. Use the to search for parameters by name or description.
- These parameters are mandatory:
- STAP\_TAP\_IP: the IP address or FQDN of the database server or node on which the STAP is being installed (equivalent to the -taphost command line parameter). If not specified, the GIM\_CLIENT\_IP value is used.
  - STAP\_SQLGUARD\_IP: the IP address or FQDN of the primary collector with which this STAP communicates (equivalent to the -appliance command line parameter). If not specified, then, the GIM\_URL value is used.
- Attention: See the enterprise load balancing parameters in [Linux-UNIX: S-TAP GIM installation parameters](#).
- Important: Unless identified as a client-specific parameter, values provided in the Choose parameters section are applied to all client installations. For client-specific parameters, the value field is disabled and values are defined per-client in the Configure clients section.
- Click Next to continue.
7. In the Configure clients section, use the table to review and edit parameter values for each client.
- Editable parameters show a icon next to the parameter value. Click the icon to edit the value.
8. Click Install to begin the software installation. Use the icon to schedule the installation, then click OK to continue.

## What to do next

Verify S-TAP status:

- In the Success popup, click Show Status to open the Status window to monitor the software install/upgrade. Click to refresh the results. If an install/upgrade has a failed status, click Uninstall if you see the button, otherwise, click Reset connection.
- View the module status in the report at Manage>Reports>Install Management>GIM Clients Status
- Verify that the row of the S-TAP has a green status (first column) in Monitor>Maintenance>S-TAP Logs>S-TAP Status

## Related concepts

- [Guardium Installation Manager](#)

## Related tasks

- [Set up by Client](#)

## Linux-UNIX: S-TAP GIM installation parameters

Understand the parameters (each with a short description) that are typically used in your GIM S-TAP agent installation.

Most parameters are also listed in [Linux-UNIX: Editing the S-TAP configuration parameters](#).

CAUTION:

Do not modify advanced parameters unless you are an expert user or IBM Technical Support advised to make the changes.

Table 1. General Parameters

| GIM parameter                | Description                                                                                                                                                                                         |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| STAP_TAP_IP                  | The IP address or FQDN of the database server or node on which the S-TAP is being installed (equivalent to the -taphost command line parameter). If not specified, the GIM_CLIENT_IP value is used. |
| STAP_SQLGUARD_IP             | The IP address or FQDN of the primary collector with which this S-TAP communicates (equivalent to the -appliance command line parameter). If not specified, then, the GIM_URL value is used.        |
| STAP_ADDITIONAL_SQLGUARD_IPS | List of space-delimited additional SQLGUARD IP addresses.                                                                                                                                           |
| STAP_ENABLED                 | Enables S-TAP when installation is complete. Default=1 (yes)                                                                                                                                        |
| STAP_FAM_ENABLED             | Enables FAM monitoring. Disabled by default. During upgrade, if the CLI parameter FAM was enabled in v10.1.4 or a prior version, then this parameter is enabled upon upgrade.                       |

| GIM parameter                  | Description                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| STAP_UPLOAD_FEATURE            | Whether or not the S-TAP uploads snapshots and new K-TAP modules to the GIM server to which it reports. Valid values: <ul style="list-style-type: none"><li>• 0: Disabled</li><li>• 1: Enabled for all (snapshots and K-TAP modules)</li><li>• 2: Enabled for snapshot; disable for K-TAP modules</li></ul>                                                                                                      |
| KTAP_ENABLED                   | Enables the K-TAP module. Default=1 (yes)                                                                                                                                                                                                                                                                                                                                                                        |
| KTAP_ALLOW_MODULE_COMBO        | Controls the FlexLoad mechanism: If the bundle does not have an exact kernel match, it installs the best match. If the K-TAP cannot be installed or does not start, a query is presented to the user whether to continue installation. Default=N                                                                                                                                                                 |
| KTAP_LIVE_UPDATE               | Enables the K-TAP update without requiring a server reboot. Default=Y                                                                                                                                                                                                                                                                                                                                            |
| GIM_ALLOW_CUSTOM_BUNDLES       | Control uploading of custom K-TAP bundle. <ul style="list-style-type: none"><li>• 0: Custom bundles are not allowed.</li><li>• 1: Allows installation of custom compiled K-TAP bundles.</li></ul> Default = 0<br>This parameter cannot be changed from the GUI or API. Only the OS Admin can change the value from 0 to 1 after GIM is installed. This parameter must be enabled on each DB server individually. |
| KTAP_PREVENT_EXACT_MATCH_BUILD | When enabled, K-TAP local builds are disabled. It is <b>not recommended</b> to enable this parameter since it decreases the possibility of finding a matching module for the running kernel.                                                                                                                                                                                                                     |
| KTAP_AIX_LOG_ROTATE_FILE_SIZE  | This parameter, together with KTAP_AIX_LOG_ROTATE_NFILES, configure the ktap.log rotation on AIX servers. When the file size reaches this threshold, in KB, it rotates. This parameter does not need modification. Valid values: >= 10. Default = 512                                                                                                                                                            |
| KTAP_AIX_LOG_ROTATE_NFILES     | The ktap.log rotation on AIX servers is enabled, by default, during installation or upgrade from previous version. This parameter specifies the maximum number of files to keep. This parameter does not need modification. Valid values: >= 2. Default=2                                                                                                                                                        |

Table 2. Enterprise Load Balancing parameters. For more information, see [Enterprise load balancing](#).

| GIM parameter                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| STAP_LOAD_BALANCER_IP            | Required if you are configuring enterprise load balancing. If blank, enterprise load balancing is disabled.<br>The IP address or hostname of the central manager or managed unit this S-TAP uses for load balancing.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| STAP_INITIAL_BALANCER_TAP_GROUP  | The name of the S-TAP group that this S-TAP belongs to, for enterprise load balancing.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| STAP_INITIAL_BALANCER_MU_GROUP   | The name of the managed unit group that the app-group is associated with. Requires a defined LB-APP-GROUP. The managed unit group must exist on the central manager before it can be used during installation of the S-TAP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| STAP_LOAD_BALANCER_NODE_AFFINITY | Whether the S-TAP connects to more than one managed unit, for enterprise load balancing. Some scenarios need all traffic to go to the same collector. With Oracle ATAP, for example, the analyzed client IP only shows if both the encrypted and unencrypted sessions go to the same managed unit. Valid values: <ul style="list-style-type: none"><li>• 0: Disabled. The S-TAP traffic goes to, at a maximum, the number of managed units specified by load_balancer_num_mus.</li><li>• 1: Enabled. The S-TAP traffic goes to one managed unit, and has, at a maximum, the number of connections (to that managed unit) specified by load_balancer_num_mus.</li></ul> See <a href="#">load_balancer_num_mus</a> |
| STAP_LOAD_BALANCER_NUM_MUS       | The number of managed units the enterprise load balancer allocates for this S-TAP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Linux-UNIX: Upgrading an S-TAP agent with GIM Setup by Client

Use the GIM tool to upgrade your S-TAP agent.

### Before you begin

Verify the following before you begin.

- The GIM client on the database server is communicating with the Guardium system.
- Obtain the S-TAP module from either [Fix Central](#), or your Guardium representative.
- Certain Guardium® Data ProtectionS-TAP updates combined with certain sniffer patches do not support the ability to transfer DB\_USER in the event of a failover. Make sure that you have installed compatible patches, as described in [Determining whether Guardium Data Protection Linux/UNIX S-TAP and Sniffer patches are compatible](#).

### About this task

- Before starting a GIM Set up by Client upgrade, you can check whether any of the database servers need to be rebooted during the S-TAP upgrade. This check is for GIM Set up by Client upgrades only; it does not cover any other upgrade scenarios. If the bundles were installed from the managed unit, run the S-TAP Agent Upgrade Pre-Check report on the managed unit. If all clients are managed by the central manager (all GIM clients point to the central manager, which is best practice and the recommended setup), run the S-TAP Agent Upgrade Pre-Check report from the central manager. The reboot status of GIM clients that point to a managed unit is not captured in a report that is run on the central manager. Verify that the GIM agent is installed on the database server before you run the report. (None of the other modules or bundles need to be installed). All database servers that are listed in the report will need reboot. Reboot is required in this scenario:
  - Upgrading with a non-live upgrade (KTAP\_LIVE\_UPGRADE=N), irrespective of whether the source and target versions are the same.
- To upgrade from a shell installed S-TAP to a GIM-controlled S-TAP: Upgrade the S-TAP using shell, to the target version. Then install the bundle-GIM STAP installer. Reboot is not required.

- In a GIM upgrade, there are two scenarios you must avoid: A-TAP users are active (causing the upgrade to fail), and maintenance is running on the databases. A typical scenario is: database server maintenance is planned for 12 midnight and you want to upgrade the S-TAP at 1AM. Use this general flow to successfully upgrade your S-TAPS.
  1. Schedule your upgrades with GIM.
  2. Disable any GIM upgrades from deploying: **configurator.sh --delayed\_bundle\_deployment enable**
  3. Wait for the database maintenance to complete.
  4. Check if A-TAP users are active (assuming the DBs are down, disable them if there are any): <GIM INSTALL DIR>/ATAP/current/files/bin/guardctl list-active
  5. Enable GIM upgrades: **configurator.sh --delayed\_bundle\_deployment disable**

## Procedure

---

1. Upload the S-TAP module for upgrade.
  - a. On the Guardium system, go to **Manage > Module Installation > Upload Modules**.
  - b. Click **Choose File** and select the S-TAP upgrade module.
  - c. Click **Upload** to upload the module to the Guardium system.  
The module is listed in the Import Uploaded Modules table.
  - d. In the Import Uploaded Modules table, click the checkbox next to the S-TAP module you want to upgrade to.  
The module is imported and made available for upgrade. After the module is imported, the Upload Modules page is reset and the Import Uploaded Modules table is empty.
2. Go to **Manage > Module Installation > Set up by Client**.
3. In the **Choose clients** section, select the database servers where you want to update software. Select individual clients with the checkboxes in the table, or use the **Select client group** menu to select a group of clients.  
Click **Next** to continue.
4. In the **Choose bundle** section, use the **Select a bundle** menu to identify your upgrade version. Click **Next** to continue.
5. Optional: You can modify the flex load mechanism with the parameter **KTAP\_ALLOW\_MODULE\_COMBOS** in the **Choose parameters** section. This parameter applies to all servers unless you specify values individually in the **Configure clients** section.
6. Click **Upgrade** to begin the software upgrade. Or use the icon to schedule the installation, then click **OK** to continue.
7. To create the Guardium API syntax for the current configuration in the **Setup by Client**, click **Generate GuardAPI**. If enough information is available, it generates API commands for multiple clients in the **GuardAPI commands** dialog. If there isn't enough information, it shows a default template.

## What to do next

---

In the Success popup, click **Show Status** to open the Status window to monitor the software upgrade. Click to refresh the results. If an upgrade has a failed status, click **Uninstall** if you see the button, otherwise, click **Reset connection**. You can also view the status of the module upgrade by reviewing the report at **Manage > Reports > Install Management > GIM Clients Status**.

Verify that the S-TAP is communicating with the Guardium system by browsing to **Manage > Activity Monitoring > S-TAP Control** and reviewing the S-TAPs status and configuration.

## Related concepts

---

- [Guardium Installation Manager](#)
- [Linux-UNIX: Working with K-TAP](#)

## Related reference

---

- [Windows: S-TAP GIM installation parameters](#)

## Linux-UNIX: Uninstalling S-TAP agent with GIM Setup by Client

---

Learn how to uninstall the S-TAP agent and the GIM bundle from the database server. If S-TAP was installed with GIM it's highly recommend to uninstall with GIM. Otherwise you would need to manually remove the S-TAP folder from the GIM directory on the DB server.

## Before you begin

---

- Verify that the GIM client on the database server is communicating with the Guardium system.
- If the database is using an exit library, disable the exit library, and then delete the exit library.
- If A-TAP is active, de-activate it before uninstalling the S-TAP. See [Linux-UNIX: A-TAP activate, deactivate and DB stop, restart guidelines](#).

## Procedure

---

1. Navigate to **Manage > Module Installation > Set up by Client**.
2. In the **Choose clients** section, select the database servers from which you are uninstalling the S-TAP. Select individual clients using check boxes in the table, or use the **Select client group** menu to select a group of clients. Click **Next** to continue.
3. In the **Choose bundle** section, select the bundle you want to uninstall from the drop-down list.  
**Tip:**
  - You can filter the clients, for example, by name, module, Selected bundle actions, and client OS. The resulting selection is persistent; **the action is applied only to the filtered list of clients**. You can see that the number of clients in the **Choose Clients** section is greater than the number in **Configure Clients** section.
  - Clear the **Show only latest versions** checkbox to view and work with earlier versions of a bundle.
  - Clear the **Show only bundles** checkbox to identify individual modules within a bundle.

- Select the Show only compatible clients checkbox to hide clients that are not compatible with the selected bundle. The Configure Clients row shows the number of clients that have that specific bundle running. Click Next to continue.
- 4. Click Uninstall. The system asks for confirmation. Click Yes.
- 5. Reboot the database server to remove K-TAP from the drivers.

## Related concepts

---

- [Guardium Installation Manager](#)

## Related tasks

---

- [Linux-UNIX: Disabling Teradata exit](#)

# Linux-UNIX: Use RPM to install, upgrade, uninstall the S-TAP

You can manage your S-TAP agent with .rpm on RHEL and for SUSE Linux databases.

- [Linux-UNIX: Installing the S-TAP agent with RPM](#)

You can install and update S-TAP on a Linux server using the RPM. The advantage of installing by RPM is that you install and maintain S-TAP using the same method that you manage all other software on the database server.

- [Linux-UNIX: S-TAP guard-config-update parameters for RPM installation and update](#)

Learn about the guard-config-update parameters used for installing an S-TAP agent, and updating its configuration.

- [Linux-UNIX: Upgrading S-TAP using RPM](#)

- [Linux-UNIX: Uninstalling S-TAP using RPM](#)

Learn how to uninstall the S-TAP agent from a Linux server using the RPM.

## Linux-UNIX: Installing the S-TAP agent with RPM

---

You can install and update S-TAP on a Linux server using the RPM. The advantage of installing by RPM is that you install and maintain S-TAP using the same method that you manage all other software on the database server.

### Before you begin

---

- Verify all [Linux-UNIX: S-TAP installation prerequisites](#).
- Obtain the correct S-TAP installer script, from either [Fix Central](#), or your Guardium representative. The script name identifies the database server operating system.
- The S-TAP shell installer does not install if there is already an RPM installed (preventing double installation).
- RPM is supported for RHEL and for SUSE Linux databases.

### About this task

---

RPM names have the format: **guard-stap-10.0.0.89165-1-rhel-6-linux-x86\_64.x86\_64.rpm**, where the first three numbers are the release number of STAP (10.0.0, 10.1.2, etc) and the fourth number is the code revision (89165). The number immediately following is the package iteration which would increment in the case of adding K-TAP modules to the RPM.

There is a single RPM for the 32-bit S-TAPs and two RPMs for the 64-bit S-TAPs so that the 64-bit S-TAP does not have a dependency on 32-bit libraries if 32-bit exit libraries are not required. The extra RPM looks like **guard-stap-32bit-exit-libs-10.1.0.89165-1-rhel-6-linux-x86\_64.x86\_64.rpm** and has a dependency on the main RPM.

By default, the installation process checks the Linux kernel to determine whether a K-TAP module has been created to work with that kernel. If it exists, it installs (sets **ktap\_installed = 1**). If there is none, K-TAP does not install unless you have enabled Loader Flexibility, which aids in the installation of currently built modules when an exact match does not exist. When Loader Flexibility is enabled, it attempts to build a K-TAP to match your Linux kernel.

RPM installs S-TAP to /opt/guardium; this location cannot be changed. **tap\_ip** is set automatically to the hostname of the system. **sqlguard\_ip** is set to 127.0.0.1 as a placeholder for proper configuration. Complete the configuration after the installation, as described in this procedure.

RPM logs are saved to /opt/guardium/rpm\_logs

You can run the **guard-config-update** script as root user or a non-root user. Use the **help** command to see your permitted functions.

## Procedure

---

1. Unzip the S-TAP package.
2. Log in to the database server as **root** and copy the RPM to /tmp.
3. To enable Loader Flexibility, set the Linux environment variable **NI\_ALLOW\_MODULE\_COMBO="Y"**. (This is particularly useful if you are using a service to push the RPMs, then you don't need to access every machine and set the parameter after installation.) Otherwise you can use the **guard-config-update** parameter **--set-flexload**.
4. Run the **rpm -i <RPM\_NAME>** command.  
The S-TAP installs.
5. Run **guard-config-update** with the **--retry-ktap-load** parameter.
6. Take one of the following steps to complete the configuration:
  - Change the directory to /opt/guardium, and running the script **guard-config-update**, using the parameters described in [Linux-UNIX: S-TAP guard-config-update parameters for RPM installation and update](#).
  - Update the S-TAP parameters in the UI. See [Linux-UNIX: Configuring S-TAP in the S-TAP Control page](#).

## What to do next

After installation completes, verify S-TAP status:

- Verify that the row of the S-TAP has a green status (first column) in Monitor > Maintenance > S-TAP Logs > S-TAP Status

## Linux-UNIX: S-TAP guard-config-update parameters for RPM installation and update

Learn about the guard-config-update parameters used for installing an S-TAP agent, and updating its configuration.

You can use the guard-config-update script to update your S-TAP configuration (without using the GUI), whether S-TAP was installed with GIM, RPM, or shell. See [Linux-UNIX: Configure S-TAP with guard-config-update](#)

Table 1. guard-config update parameters

| Parameter                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --stap-dir                                    | S-TAP install directory if not default (default: /usr/local/guardium).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| --migrate-to-insights [tenant ID] [routeName] | Migrate an S-TAP to Guardium® Insights. Parameters:<br><br>tenant ID<br>The Guardium Insights tenant ID, including the <i>TNT_</i> prefix.<br>routeName<br>The DNS hostname for the Guardium Insights deployment. The DNS hostname is the same as the URL for the UI (without the https:// prefix).<br><br>Note: Before migrating the S-TAP, Guardium Insights must have a signed, trusted certificate that the S-TAP can locate. Store the certificate either in the default location ( <code>INSTALL_DIR/etc/pki/certs/trusted/ca.cert.pem</code> , where <code>INSTALL_DIR</code> is the Guardium Data Protection installation directory or configure a different location in the <code>guard_tap.ini</code> by using the <code>guardium_ca_path</code> parameter. If you specify a custom location, you must manually store the certificate (that is, you cannot use the <code>push_insights_trust</code> API). You can also use the <code>migrate_stap_config</code> API to migrate S-TAPs. |
| --set-tap-ip [IP or hostname]                 | Set <code>tap_ip</code> in S-TAP config file <code>/usr/local/guardium/guard_stap/guard_tap.ini</code> (default: <code>rh5u9x64t.guard.swg.usma.ibm.com</code> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| --set-sqlguard-ip [IP or hostname]            | Set <code>sqlguard_ip</code> in SQLGuard_0 section in S-TAP config file <code>/usr/local/guardium/guard_stap/guard_tap.ini</code> (default: <code>127.0.0.1</code> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| --add-sqlguard [ID] [IP or hostname]          | Add SQLGuard_ID section to S-TAP config file <code>/usr/local/guardium/guard_stap/guard_tap.ini</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| --remove-sqlguard [ID]                        | Remove SQLGuard_ID section from the S-TAP config file. <code>/usr/local/guardium/guard_stap/guard_tap.ini</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| --modify-sqlguard [ID] [parameter] [value]    | Set SQLGuard_ID section parameter to value in S-TAP config file <code>/usr/local/guardium/guard_stap/guard_tap.ini</code> . Parameters:<br><br><code>sqlguard_ip</code><br>IP address or hostname of SQLGuard unit<br><br><code>sqlguard_port</code><br>Port used to connect to SQLGuard unit (default: 16016)<br><br><code>primary</code><br>Order of preference (1=primary, 2=secondary, 3=tertiary, and so on)<br><br><code>num_main_thread</code><br>Number of main connections to use for this SQLGuard, used with <code>participate_in_load_balancing = { 1, 4 }</code> (default: 1)<br><br><code>connection_pool_size</code><br>Number of data connections per main connection to SQLGuard unit (default: 0)                                                                                                                                                                                                                                                                              |
| --modify-tap [parameter] [value]              | Set TAP section parameter to value in S-TAP config file <code>/usr/local/guardium/guard_stap/guard_tap.ini</code> . For the list of <code>guard_tap.ini</code> parameters, see <a href="#">guard_tap.ini parameters</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| --help-config [option]                        | Show information about an option in the ini, if available (show all available if none specified).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| --set-flexload [0 or 1]                       | Controls the K-TAP FlexLoad mechanism: 0: disable, 1: enable.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| --retry-ktap-load                             | Retry K-TAP loading (useful after installing dev packages, updating after K-TAP request, or changing flexload; automatically restarts S-TAP).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| --discover-ies                                | Run discovery and replace all Inspection Engines with those discovered.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| --stop [service]                              | Stop service (S-TAP, or monitor) temporarily (Solaris services and inittab treat this as permanent disable, does not auto-start on boot until re-enabled).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| --start [service]                             | Start service (S-TAP, or monitor) if not already running (implies enable).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| --restart [service]                           | Restart service (S-TAP, or monitor) if already running.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| --disable [service]                           | Prevent service (S-TAP, or monitor) from running again.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| --enable [service]                            | Configure service (S-TAP, or monitor) for automatic start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| --status                                      | Show which services are started and if they are configured to start automatically.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Parameter                            | Description                                                                                                                                     |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| --show-tap [option]                  | Shows the value that is currently stored for a parameter in the TAP section of the guard_tap.ini file.                                          |
| --show-ies                           | Shows the currently configured inspection engines in the guard_tap.ini file.                                                                    |
| --set-ktap-prevent-exact-match-build | Enable or disable the K-TAP local build. It is recommended to leave the KTAP local build enabled, which is the default setting when installing. |

Table 2. guard.\_tap.ini parameters

| Parameter                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| all_can_control                   | Defines which Guardium system controls this S-TAP. Valid values: <ul style="list-style-type: none"><li>• 0: S-TAP is controlled by the primary Guardium system only.</li><li>• 1: S-TAP can be controlled by any Guardium system.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| tap_debug_output_level            | Set debugging level (must be an integer >= 0, but not 2 or 3). See <a href="#">tap_debug_output_level</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| participate_in_load_balancing     | Set participate in load balancing (values: 1, 2, 3, 4). (See <a href="#">Linux-UNIX: S-TAP load-balancing models and configuration guidelines</a> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| use_tls                           | Enable TLS (0: no, 1: yes).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| hunter_trace                      | Enable UID chain reporting (0: no, 1: yes).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| buffer_file_size                  | Buffer file size in MB.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| alternate_ips                     | Comma-separated list of alternate IPs/hostnames for S-TAP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| firewall_installed                | Enable firewall (0: no, 1: yes).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| firewall_fail_close               | Action to take when there is no verdict (for example, SQLGuard unreachable or timeout reached) (0: do nothing, 1: block connection)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| firewall_default_state            | Set default state (0: not watched, 1: watched)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| firewall_timeout                  | Set firewall timeout in seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| firewall_force_watch              | Comma-separated list of IP/masks to watch even with firewall_default_state=0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| firewall_force_unwatch            | Comma-separated list of IP/masks to unwatch even with firewall_default_state=1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| qrw_installed                     | Enable or disable the query rewrite feature. When set to 0, all other parameters in this group are ignored. Valid values: <ul style="list-style-type: none"><li>• 0: Disabled</li><li>• 1: Enabled</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| qrw_default_state                 | Sets the query rewrite activation trigger. Must be 0 if firewall_default_state=1. Valid values: <ul style="list-style-type: none"><li>• 0: QRW activated per session when triggered by a rule in the installed policy</li><li>• 1: QRW activated for every session regardless of the installed policy</li><li>• 2: All traffic is watched by default for QRW policy violations, but if no event triggers the watch in the first PRIORITY_COUNT packets, query rewrite is turned off for the session.<br/>When set to 2, the QRW operation can be modified by the commands: Watch, Drop, Watch &amp; Drop and Unwatch. When a watch command is received while state 2 is in effect, it changes the state from 2 to 1 so that the connection is permanently subject to firewall or query rewrite operations. When a Drop or Watch &amp; Drop is received, the connection is immediately terminated. When an unwatch command is received while state 2 is in effect, it changes the state from 2 to 0 so the connection is no longer subject to firewall or query rewrite operations.</li></ul> |
| qrw_force_watch                   | Comma-separated list of client IP/MASKs (for example, 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2) to watch automatically. Valid when qrw_installed is 1, and qrw_default_state is 0. Cannot be configured to the same IP range as firewall_force_watch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| qrw_force_unwatch                 | Comma-separated list of client IP/MASKs (for example, 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2) to exclude from watching. Valid when qrw_installed is 1, and qrw_default_state is 1. Cannot be configured to the same IP range as firewall_force_unwatch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| server_side_masking_installed     | Enables the server-side masking feature. Valid values: <ul style="list-style-type: none"><li>• 0=No</li><li>• 1=Yes</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| server_side_masking_default_state | Sets the server-side masking activation trigger. Valid values: <ul style="list-style-type: none"><li>• 0=SSM activated per session when triggered by a rule in the installed policy.</li><li>• 1=SSM activated for every session regardless of the installed policy.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| server_side_masking_default_state | Sets the server-side masking activation trigger. Valid values: <ul style="list-style-type: none"><li>• 0=SSM activated per session when triggered by a rule in the installed policy.</li><li>• 1=SSM activated for every session regardless of the installed policy.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| server_side_masking_force_watch   | Comma separated list of client IP/MASKs (for example, 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2) whose sessions are watched automatically. Valid when server_side_masking_installed=1 and qrw_default_state=0.<br>Cannot be configured to the same range as firewall_force_watch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| server_side_masking_force_unwatch | Comma separated list of client IP/MASKs (for example, 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2) whose sessions are not watched. Valid when server_side_masking_installed is 1 and firewall_default_state is 1.<br>Cannot be configured to the same range as firewall_force_unwatch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Parameter                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| db_request_handler_enable             | Allow the database to access K-TAP without manual configuration (requires a defined db_user in the IE section). Valid values: <ul style="list-style-type: none"> <li>• 0: Disabled</li> <li>• 1: Enabled</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                |
| fam_enable                            | Global enable/disable for FAM. Valid values: <ul style="list-style-type: none"> <li>• 0: Disabled</li> <li>• 1: Enabled</li> </ul> <p>FAM rules must be defined in order for FAM to run. If rules are not defined, enabling this parameter opens a connection to the Guardium system on port 16022 (or 16023 if using encryption), but FAM remains essentially disabled.</p>                                                                                                                                                                                                                       |
| kafka_reader_enabled                  | Enables Cloudera Navigator integration using Kafka publish and consume. Valid values: <ul style="list-style-type: none"> <li>• 0: Disabled</li> <li>• 1: Enabled</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                        |
| kafka_bootstrap_servers               | Required. The comma separated list of host_name:port pairs are used to establish the initial connection to the Kafka cluster. After the initial connection is established, all servers in the cluster are used. Consider specifying more than one bootstrap in case one is down. Example:<br>hostnameofbroker1:9092,hostnameofbroker2:9092.                                                                                                                                                                                                                                                        |
| kafka_topic_name                      | Required. The topic name in the Kafka cluster that Cloudera publishes audits to, and that S-TAP reads audits from.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| kafka_group_name                      | Required. Assigns the S-TAP to this Kafka consumer group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| kafka_ssl_ca_location                 | Required if kafka_use_tls = 1. Path to the certificate authority (CA) for verifying the Kafka cluster certificate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| kafka_debug                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| kafka_extra_config                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| force_server_ip                       | Forces the reported server IP of the database to be the value stored in tap_ip. Valid values: <ul style="list-style-type: none"> <li>• 0: Disabled</li> <li>• 1: Enabled</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                |
| tenant_id                             | To use an S-TAP with Guardium Insights, the Guardium Insights tenant ID is required, including the TNT_ prefix. For example:<br><b>tenant_id=TNT_N5YBRAPBWRYAPFLQWABCDE</b>                                                                                                                                                                                                                                                                                                                                                                                                                        |
| enable_dynamic_ring_buffers           | Dynamically adds and removes S-TAP buffers for each main connection during peak traffic to prevent an overflow in the S-TAP buffer. If S-TAP failover happens, data in all buffers is moved to the new buffers.<br>Valid values: <ul style="list-style-type: none"> <li>• 0: Disabled</li> <li>• 1: Enabled</li> </ul>                                                                                                                                                                                                                                                                             |
| enable_ktap_dynamic_ring_buffers      | Dynamically adds and removes K-TAP buffers for each main connection during peak traffic, to prevent an overflow in the K-TAP buffer. If K-TAP failover happens, data in all buffers is moved to the new buffers.<br>Valid values: <ul style="list-style-type: none"> <li>• 0: Disabled</li> <li>• 1: Enabled</li> </ul>                                                                                                                                                                                                                                                                            |
| enable_stap_soft_restart              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| buffer_percentage_for_priority_packet | Allows you to adjust the buffer percentage for priority packets. Increasing the value reserves more space for priority packets.<br>When Guardium reaches the buffer usage maximum (that is, 100% - buffer_percentage_for_priority_packet, non-priority packets are dropped to help ensure that priority packets get through.<br>The range is 1 (1%, the default) to 5 (5%).                                                                                                                                                                                                                        |
| use_exit_db_type                      | Allows database auto-discovery to discover any databases that have Exit protocols and add those instances to Discovered Instances report.<br>Valid values: <ul style="list-style-type: none"> <li>• 0: Do not autodiscover databases that have Exit protocols.</li> <li>• 1: Discover databases that have Exit protocols. For more information, see <a href="#">Using Exit discovery</a>.</li> </ul>                                                                                                                                                                                               |
| db_exit_list                          | Discover databases that are supported with Exits. When an Exit database type is discovered, K-TAP is automatically disabled.<br>When use_db_exit is set to 0, this parameter is ignored.<br>Valid values (when use_db_exit is set to 1): <ul style="list-style-type: none"> <li>• All - Discovery discovers databases supported with Exit along with other non-Exit databases.</li> <li>• None: Discovery does not discover any databases with Exits.</li> <li>• &lt;DB type&gt; : Discovery discovers only the specified database. DB type can be: DB2, INFORMIX, NETEZZA, or TERADATA</li> </ul> |
| stap_buf_mem_percent                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Parameter                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| load_balancer_node_affinity          | Whether the S-TAP connects to more than one managed unit, for enterprise load balancing. Some scenarios need all traffic to go to the same collector. With Oracle ATAP, for example, the analyzed client IP only shows if both the encrypted and unencrypted sessions go to the same managed unit. Valid values: <ul style="list-style-type: none"> <li>• 0: Disabled. The S-TAP traffic goes to, at a maximum, the number of managed units specified by load_balancer_num_mus.</li> <li>• 1: Enabled. The S-TAP traffic goes to one managed unit, and has, at a maximum, the number of connections (to that managed unit) specified by load_balancer_num_mus</li> </ul> See <a href="#">load_balancer_num_mus</a> . |
| guardium_ca_path                     | Location of the Certificate Authority certificate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| sqlguard_cert_cn                     | The common name to expect from the Sqlguard certificate                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| initial_balancer_mu_group            | The managed unit group name to associate with this S-TAP (by the central manager load balancer) when installing an S-TAP. The group name is sent with each request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| initial_balancer_tap_group           | The S-TAP group name to associate with this S-TAP (by the central manager load balancer) when installing an S-TAP. The group name is sent with each request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| load_balancer_recheck_interval       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| transmit_session_losses_metadata     | Determines whether to create a SessionLossesMetadata message that report metadata if packets are dropped for a given session. Valid values: <ul style="list-style-type: none"> <li>• 0 (disabled). Do not send the SessionLossesMetadata message.</li> <li>• 1 (enabled). Send the SessionLossesMetadata, but only when a new collector is found.</li> </ul>                                                                                                                                                                                                                                                                                                                                                         |
| discovery_ora_use_port_ranges        | Enable S-TAP discovery of Oracle databases to combine discovered instances based on port ranges. This setting works with a single unix_domain_socket_marker. Multiple unix_domain_socket_marker configurations require separate instances. Valid values: <ul style="list-style-type: none"> <li>• 0: disabled</li> <li>• 1: enabled</li> </ul>                                                                                                                                                                                                                                                                                                                                                                       |
| global_session_key                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| internal_load_balancer_time_interval |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## Linux-UNIX: Upgrading S-TAP using RPM

### Before you begin

Obtain the correct S-TAP installer script, from either [Fix Central](#), or your Guardium representative. The script name identifies the database server operating system. Note: Certain Guardium® Data ProtectionS-TAP updates combined with certain sniffer patches do not support the ability to transfer DB\_USER in the event of a failover. Make sure that you have installed compatible patches, as described in [Determining whether Guardium Data Protection Linux/UNIX S-TAP and Sniffer patches are compatible](#).

### About this task

RPM names have the format: **guard-stap-10.6.0.0.89165-1-rhel-6-linux-x86\_64.x86\_64.rpm**, where the first three numbers are the release number of STAP (10.0.0, 10.1.2, etc) and the fourth number is the code revision (89165). The number immediately following is the package iteration which would increment in the case of adding K-TAP modules to the RPM.

There is a single RPM for the 32-bit S-TAPs and two RPMs for the 64-bit S-TAPs so that the 64-bit S-TAP does not have a dependency on 32-bit libraries if 32-bit exit libraries are not required. The extra RPM looks like **guard-stap-32bit-exit-libs-10.1.0.89165-1-rhel-6-linux-x86\_64.x86\_64.rpm** and has a dependency on the main RPM.

RPM logs are saved to /opt/guardium/rpm\_logs

You can run the guard-config-update script as root user or a non-root user. Use the help command to see your permitted functions.

All S-TAP configuration persists during the upgrade.

### Procedure

1. Unzip the S-TAP package and copy the RPM to /opt/guardium of the database server.
2. Run the command: `rpm -U <RPM_NAME>`. If you want to modify the FlexLoad mechanism value, include the parameter in the rpm command: --set-flexload, where 0 disables the feature, and 1 enables it.

### What to do next

After the upgrade completes, verify S-TAP status:

- Verify that the row of the S-TAP has a green status (first column) in Monitor > Maintenance > S-TAP Logs > S-TAP Status

## Related concepts

---

- [Linux-UNIX: S-TAP compilation of K-TAP](#)

## Related reference

---

- [Linux-UNIX: S-TAP guard-config-update parameters for RPM installation and update](#)

# Linux-UNIX: Uninstalling S-TAP using RPM

Learn how to uninstall the S-TAP agent from a Linux server using the RPM.

## Before you begin

---

- If the database is using an exit library, disable the exit library, and then delete the exit library.
- If A-TAP is active, de-activate it before uninstalling the S-TAP. See [Linux-UNIX: A-TAP activate, deactivate and DB stop, restart guidelines](#).

## Procedure

---

1. To get the RPM name, run: `rpm -qa | grep guard_stap`
2. Run `rpm -e <RPM_NAME>`

## Results

---

After uninstalling S-TAP, the directory /opt/guardium still exists, but should only contain /opt/guardium/guard\_stap/guard\_tap.ini.rpmsave and /opt/guardium/rpm\_logs.

## Related tasks

---

- [Linux-UNIX: Disabling Teradata exit](#)

# Linux-UNIX: Use shell installer to install, upgrade, uninstall the S-TAP

- [Linux-UNIX: Installing the S-TAP client by using the shell installer](#)  
Use the shell installer, either in interactive mode or non-interactive mode, to install the S-TAP client on Linux, Solaris, HPUX, and AIX database servers.
- [Linux-UNIX: S-TAP install script parameters](#)  
Understand the guard-stap-setup script for installing an S-TAP.
- [Linux-UNIX: Upgrading the S-TAP agent using the shell installer](#)  
Use the shell installer, either in interactive mode or non-interactive mode, to upgrade the S-TAP agent on Linux, Solaris, HPUX, and AIX database servers.
- [Linux-UNIX: Uninstalling S-TAP agents using the shell installer](#)  
Perform this procedure before installing a new version of S-TAP if you want to save the old configuration file.
- [Linux-UNIX: Converting a shell managed S-TAP to a GIM managed S-TAP](#)  
An S-TAP that was installed by shell can be converted to a GIM-managed S-TAP.

# Linux-UNIX: Installing the S-TAP client by using the shell installer

Use the shell installer, either in interactive mode or non-interactive mode, to install the S-TAP client on Linux, Solaris, HPUX, and AIX database servers.

## Before you begin

---

- Verify all [Linux-UNIX: S-TAP installation prerequisites](#).
- Obtain the correct S-TAP installer script, from either [Fix Central](#), or your Guardium representative. (The installation fails if the version is incorrect.) The script name identifies the database server operating system. The S-TAP package name is in the format: `guard-stap-10.6.0.0_r123456_1-rhel-5-linux-x86_64.sh`, where the first three numbers are the release number, followed by the revision number, in this example r123456.
- Alternately, download the consolidated installer that contains support for all versions for a particular operating system. For example, `guard-stap-11.4.0.0_r110473_trunk_1-suse.sh` can install any suse system of any version or CPU. These packages are much larger than the version-specific packages, though.

## About this task

---

Interactive mode must be run individually on each system, and is therefore recommended for individual S-TAPs. It provides validation at each step, which means less chance of errors. It is useful for smaller deployments or whenever a guided, step-by-step installation experience is required. The system prompts for the basic configuration, and verifies your input immediately, so that the installation does not result in errors.

By default, K-TAP is installed automatically during S-TAP installation. The S-TAP installer checks if the K-TAP is available for the kernel version. If the installation process does not find a matching K-TAP, it attempts to build one to match your Linux kernel. If the K-TAP cannot be installed or does not start, a query is presented to the user whether to continue installation. See [Linux-UNIX: Working with K-TAP](#).

If /tmp is mounted with the `noexec` option, you can set the shell variable TMPDIR to some other directory that is not mounted `noexec` (typically ~/tmp). For example, `TMPDIR=~/tmp` `/var/tmp/guard-stap-11.1.0.0_r107068_trunk_1-ubuntu-18.04-linux-x86_64.sh`.

If any stage of the installation fails, undo all of the steps up to that point. Do not leave the S-TAP partially installed.

## Procedure

---

1. Log on to the database server using the `root` account. (S-TAP must always be installed by root.)
2. Designate an installation directory and verify it has sufficient disk space, approximately 400 MB - 500 MB total.
3. Copy the S-TAP installer to the local disk on the database server, typically to `/tmp`.
4. For interactive mode, run the installer script.

```
./guard-stap-guard-<release number>_<revision number>_1-rhel-5-linux-x86_64.sh
```

The only value that you must enter is the IP address of your Guardium collector, or the collector name. All other values can be left at their defaults. The installer typically prompts as follows.

```
Enter the path prefix [/usr/local]?
Directory /usr/local/guardium/guard_stap does not exist, would you like to create it? [Y/n]
System library path [/usr/lib]?
Run STAP as root, or as user 'guardium'? [R/u]
Install STAP as root, or as user 'guardium'? [r/U]
Would you like to run guard_discovery? [Y/n]
Do you want to configure load balancer functionality? [y/N]
IP address of the SQL Guard unit:
Do you want to edit the parameters file? [y/N]
```

```
If you later update your kernel to another version, we can
try to load the closest fitting delivered module. This
feature is not enabled by default, but we recommend enabling
it to reduce delays in support. Note that if all the
packages require to build natively are installed, a local
build to generate an exact matching module will be attempted
prior to looking for non-exact matches.
Do you wish to enable this feature (y/N/h)?
```

If you choose yes to the prompt Would you like to run guard\_discovery? [Y/n], then it runs the guard\_discovery once with the --update-tap-flag to initially configure inspection engines. No matter what, it configures guard\_discovery --send-to-sqlguard-flag to run once every 24 hours.

5. For non-interactive mode, enter a command similar to this one, which uses the minimum parameters:

```
./guard-stap-guard-<release number>_<revision number>_1-rhel-5-linux-x86_64.sh -- --ni --dir
<guardium_installation_directory> --tapip <tap_ip or host_name> --sqlguardip <sqlguard_ip or host_name>
```

See the parameter description in [Linux-UNIX: S-TAP install script parameters](#).

## What to do next

---

Verify that the row of the S-TAP has a green status (first column) in Monitor > Maintenance > S-TAP Logs > S-TAP Status

## Linux-UNIX: S-TAP install script parameters

---

Understand the guard-stap-setup script for installing an S-TAP.

### Install script command line syntax

```
Usage guard-stap-setup [options]
```

Example

```
./guard-stap-guard-<release number>_<revision number>_1-rhel-5-linux-x86_64.sh -- --ni --dir <guardium_installation_directory>
--tapip <tap_ip or host_name> --sqlguardip <sqlguard_ip or host_name>
```

| Parameter               | Usage                                                                                                                                                                                         |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --?                     | Help - displays commands and their descriptions                                                                                                                                               |
| --ni                    | Non-interactive install.                                                                                                                                                                      |
| -k   -p                 | Specify whether to install with K-TAP (-k) or to not install K-TAP (-p) when K-TAP is not required (such as when using an Exit).                                                              |
| --ignore-compat         | Ignore script compatibility check.                                                                                                                                                            |
| -u                      | Update if a previous installation is found.                                                                                                                                                   |
| --user   --root         | Run S-TAP as user or root.<br>For more information about how to define these parameters, see <a href="#">Linux-UNIX: Before you start installing S-TAP</a> .                                  |
| --userinst   --rootinst | Install S-TAP as user or root.<br>For more information about how to define these parameters, see <a href="#">Linux-UNIX: Before you start installing S-TAP</a> .                              |
| --overwrite-existing    | Overwrite the existing installation if found. This parameter is disabled by default. If you specify it in an install or upgrade, it is disabled again after the install or upgrade completes. |
| --libdir <library>      | System library path. The library files must be located in a directory that is configured as trusted by the system. For example, /usr/lib on Linux, even on 64-bit systems. Default = /usr/lib |
| --tls force   none      | S-TAP TLS setting. The failover option is deprecated from v10.5.                                                                                                                              |
| --dir <dir>             | S-TAP install directory.                                                                                                                                                                      |

| Parameter                                     | Usage                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --ipfile <file>                               | <p>Text file that specifies a list of hostnames, IP addresses, and Guardium system addresses separated by a single space. For example:</p> <pre>database-01 10.10.10.1 gmachine-01 database-02 10.10.10.2 gmachine-01 database-03 10.10.10.3 gmachine-02</pre> <p>The command would look like:<code>/var/tmp/guard-stap-10.0.0_r103368_v10_5_1-rhel-5-linux-x86_64.sh --ni --dir /usr/local --ipfile /var/tmp/ipfile.txt</code></p> <p>GIM is a much easier way of configuring these parameters.</p> |
| --tapi <tapi>                                 | The IP of the machine S-TAP is being installed on.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| --sqlguardip <sqlguardip>                     | The IP of the Guardium system this S-TAP should communicate with.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| --presets <file>   <preset-options>           | Read installation settings or write them to a file.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| --no-discovery                                | Do not use the discovery utility to configure inspection engines. This parameter is disabled by default. If you specify it in an install or upgrade, it is disabled again after the install/upgrade completes.                                                                                                                                                                                                                                                                                       |
| --modules <module-bundles>                    | Specify an external K-TAP modules bundle.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| --ktap_allow_module_combos                    | Controls the FlexLoad mechanism: Allow inexact kernel match for K-TAP loading. If the bundle does not have an exact kernel match, it installs the best match. This parameter is disabled by default. If you specify it in an install or upgrade, it is disabled again after the install/upgrade completes.                                                                                                                                                                                           |
| --ktap_prevent_exact_match_build              | When specified, disables the K-TAP local build. It is <b>not recommended</b> to set this parameter; it increases the likelihood of not being able to find a matching module for the running kernel. This parameter is disabled by default. If you specify it in an install or upgrade, it is disabled again after the install/upgrade completes.                                                                                                                                                     |
| --ktap_log_rotate_file_size <file size in KB> | This parameter, together with KTAP_AIX_LOG_ROTATE_NFILES, configure the ktap.log rotation on AIX servers. When the file size reaches this threshold, in KB, it rotates. This parameter does not need modification. Valid values: >= 10. Default = 512                                                                                                                                                                                                                                                |
| --ktap_log_rotate_n_files                     | The ktap.log rotation on AIX servers is enabled, by default, during installation or upgrade from previous version. This parameter specifies the maximum number of files to keep. This parameter does not need modification. Valid values: >= 2. Default=2                                                                                                                                                                                                                                            |
| --load-balancer-ip <load_balancer_ip>         | The IP address of the central manager or managed unit this S-TAP uses for enterprise load balancing.                                                                                                                                                                                                                                                                                                                                                                                                 |
| --lb-app-group <app_group>                    | The application group name that this S-TAP belongs to for enterprise load balancing.<br>Attention: Group names with spaces or special characters are not supported.                                                                                                                                                                                                                                                                                                                                  |
| --lb-mu-group <mu_group>                      | The Managed Unit group name the app-group is associated with. Requires a defined LB-APP-GROUP. Define the MU group on the central manager before installing the S-TAP.<br>Attention: Group names with spaces or special characters are not supported.                                                                                                                                                                                                                                                |
| --lb-num-mus <number_of_mus>                  | The number of managed units the enterprise load balancer allocates for this S-TAP.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| --fam-enable                                  | Enables or disables FAM. FAM rules must be defined in order for FAM to run. If rules are not defined, enabling this parameter opens a connection to the Guardium system on port 16022 (or 16023 if using encryption), but FAM remains essentially disabled.<br>Default value: 0<br><br>If this parameter is present in the script arguments, then the fam_enable is set to 1.                                                                                                                        |
| --fam-installed                               | Valid values: 0 and 1.<br>0: FAM module will not be installed.<br><br>1: FAM module will be installed<br><br>Default value: 0                                                                                                                                                                                                                                                                                                                                                                        |
| --skip-third-party-check                      | If Guardium detects a third-party conflict, K-TAP installation can fail during a shell installation. When this parameter is set, the S-TAP install process does not check for third-party applications, but sends the following warning:<br><br><code>KTAP MODULE WARNING OVERRIDE is enabled ... skipping third party kernel extension check</code>                                                                                                                                                 |

## Linux-UNIX: Upgrading the S-TAP agent using the shell installer

Use the shell installer, either in interactive mode or non-interactive mode, to upgrade the S-TAP agent on Linux, Solaris, HPUX, and AIX database servers.

### Before you begin

- Obtain the correct S-TAP bundle, from either [Fix Central](#), or your Guardium representative. The script name identifies the database server operating system.
- Certain Guardium® Data ProtectionS-TAP updates combined with certain sniffer patches do not support the ability to transfer DB\_USER in the event of a failover. Make sure that you have installed compatible patches, as described in [Determining whether Guardium Data Protection Linux/UNIX S-TAP and Sniffer patches are compatible](#).

### About this task

If any stage of the upgrade fails, undo all of the steps up to that point. Do not leave the S-TAP partially upgraded.

The S-TAP package name is in the format: `guard-stap-11.0.0.0_r123456_1-rhel-5-linux-x86_64.sh`, where the first three numbers are the release number, followed by the revision number, in this example r123456.

## Procedure

---

1. Log on to the database server using the `root` account.
2. Copy the S-TAP bundle to the installation directory, and run the command: `./guard-stap-guard-<release number>_<revision number>_1-rhel-5- linux-x86_64.sh`. If you want to enable the FlexLoad mechanism setting, include the parameter: `ktp_allow_module_combos`  
If you are running the script interactively, without the `-u` parameter, the system responds:  

```
Do you want to update the previous STAP installation? [y/N]
```

If you're running non-interactively (`-ni`) without the `-u` parameter, the system responds with this error:  

```
Detected previous STAP installation Run installer with '-u' flag to update previous installation
```
3. Confirm you want to upgrade. The script runs, and at completion you should see output similar to: Successfully updated from 10.6.0.0 105601 to 11.0.0.0 105854

## What to do next

---

Verify that the row of the S-TAP has a green status (first column) in Monitor > Maintenance > S-TAP Logs > S-TAP Status

## Linux-UNIX: Uninstalling S-TAP agents using the shell installer

---

Perform this procedure before installing a new version of S-TAP if you want to save the old configuration file.

### Before you begin

---

- If the database is using an exit library, disable the exit library, and then delete the exit library.
- If A-TAP is active, de-activate it before uninstalling the S-TAP. See [Linux-UNIX: A-TAP activate, deactivate and DB stop, restart guidelines](#).

### About this task

---

If you have installed A-TAP, you must deactivate it before attempting any upgrade/install operations; see the description of the A-TAP deactivation command, in [Linux-UNIX: Deactivating A-TAP](#).

If you are removing a previous version of S-TAP that used K-TAP, this procedure includes rebooting the database server. If K-TAP has been installed, you have a device file named: `/dev/guard_ktap`.

## Procedure

---

1. Log on to the database server system using the `root` account.
2. Optionally, copy the S-TAP configuration file to a safe location (a non-Guardium directory). By default, the full path name is: `/usr/local/guardium/guard_stap/guard_tap.ini`.  
You can use this file later if you have to re-install this version of the software, or you can refer to it when configuring an updated version of S-TAP. Do not ever use an older configuration file directly with a newer version of the software - newer properties may be missing, and the defaults taken may result in unexpected behavior when you start S-TAP.
3. Run the uninstall script. For example, if the default directory has been used: `[root@yourserver ~]# /usr/local/guardium/guard_stap/uninstall`
4. If your previous version of S-TAP included K-TAP, reboot the database server now.

### Related tasks

---

- [Linux-UNIX: Disabling Teradata exit](#)

## Linux-UNIX: Converting a shell managed S-TAP to a GIM managed S-TAP

---

An S-TAP that was installed by shell can be converted to a GIM-managed S-TAP.

### Before you begin

---

Verify that:

- S-TAP is up and running.
- K-TAP is loaded.
- Database activities are captured.
- Download the BUNDLE-GIM and save it on the database server.

### About this task

---

If you use the BUNDLE-GIM and BUNDLE-STAP that have the exact same version and revision number as the S-TAP, you do not need to reboot the database server. You can upgrade the S-TAP by installing a higher version or revision of the BUNDLE-STAP, but you need to reboot the database server.

## Procedure

---

1. Copy the GIM client installer on the database server in any folder.
2. Install the GIM client on database server where S-TAP is running by using the downloaded GIM client shell installer script.  
For example:  
If the GIM client reports to the same collector as the S-TAP:  

```
./guard-bundle-GIM-X.X.X_rXXXX_v1X_1-rhel-8-linux-x86_64.gim.sh -- -q
```

If the GIM client reports to the central manager:  

```
./ guard-bundle-GIM-X.X.X_rXXXX_v1X_1-rhel-8-linux-x86_64.gim.sh -- --sqlguardip <CM_IP> -q
```

The database responds:  

```
Installing modules
Installation completed successfully
```
3. Verify that the GIM and SUPERVISOR processes are running by entering the command:  

```
ps -ef|grep modules
```
4. Log in to the Guardium system that this S-TAP reports to. Go to Manage->Module Installation->Set up by Client.
5. In the Choose clients section, select the clients using check boxes in the table. Click Next to continue.
6. In the Choose bundle section, use the Select a bundle menu to select the bundle that is installed on the database.
7. Click Next, the click Install, and then click now or OK  
Allow about 5 minutes for installation to finish.
8. Verify the installation status in the GIM Events List report.  
If you used the exact same version and revision number of BUNDLE-GIM and BUNDLE-STAP as the currently running S-TAP on the database server, then S-TAP and K-TAP continue to monitor database activities but are managed by GIM. The Event description column in the GIM Events List report should show Status: OK
9. If you upgraded the S-TAP by installing a higher version or revision of BUNDLE-STAP, verify that the Event description column in the GIM Events List report is IP-PR.  
Reboot the database server as follows, depending on the operating system.
  - AIX: reboot
  - Linux® shutdown -r
  - SuSe: reboot
  - HP-UX: shutdown -r
  - Solaris: shutdown -i [6|0] (Note: '0' can be used only if shutdown is done from the terminal server)

## Linux-UNIX: Use native installers to install, upgrade, uninstall the S-TAP

---

The native installer provides a shell for the shell installer. The only advantage is that it ensures that S-TAP is registered in the operating system asset repository. This registration is not required by Guardium® for the installation of the S-TAP, but it might be a requirement at your company. Use the native installer only when necessary.

A native installer ensures that S-TAP is registered in the operating system asset repository. This registration is not required by Guardium for the installation of the S-TAP, but it might be a requirement at your company. There is a separate native installer for each OS type.

- [Linux-UNIX: Installing and uninstalling S-TAP with AIX native installer](#)
- [Linux-UNIX: Installing and uninstalling S-TAP with HP-UX native installer](#)
- [Linux-UNIX: Installing and uninstalling the S-TAP with Solaris native installer](#)

## Linux-UNIX: Installing and uninstalling S-TAP with AIX native installer

---

### Before you begin

---

- Verify all [Linux-UNIX: S-TAP installation prerequisites](#).
- Obtain the correct native installer file (.bff file), from either [Fix Central](#), or your Guardium representative.

## Procedure

---

1. Obtain the IP address of the database server on which you are installing S-TAP. If virtual IPs are used, note those as well (you will need to configure those later, when completing the configuration).
2. Identify the IP address of the collector that will control this S-TAP, and to which this S-TAP will report and verify connectivity between the database server and the collector..
3. Copy the S-TAP installer to the local disk on the database server, typically to /tmp.
4. Enter the following command on a clean server (no previous S-TAP installation) to extract the shell installer for AIX®, substituting the appropriate file name with the appropriate .bff file:

```
installp -ax -d/var/tmp<filename> SqlGuardInstaller
Example:
installp -ax -d/var/tmp/guard-stap-guard-8.0.00rc1_r20934_1-aix-5.2-aix-powerpc.bff SqlGuardInstaller
```

The shell installer that is extracted, named guardium, is under /usr/local.

5. Continue with [running the interactive installer](#) of the installation procedure, running the generated installation script rather than the default installation script for the operating system version.

## Remove AIX S-TAP using Native Installer

---

### Procedure

To remove AIX S-TAP using the native installer:

```
/usr/lib/instl/sm_inst installp_cmd -u -f 'filename'
Example
/usr/lib/instl/sm_inst installp_cmd -u -f'SqlGuardInstaller'
```

## Linux-UNIX: Installing and uninstalling S-TAP with HP-UX native installer

### Before you begin

- Verify all [Linux-UNIX: S-TAP installation prerequisites](#).
- Obtain the correct native installer file (.depot.gz file), from either [Fix Central](#), or your Guardium representative.

### Procedure

1. Obtain the IP address of the database server on which you are installing S-TAP. If virtual IPs are used, note those as well (you will need to configure those later, when completing the configuration).
2. Identify the IP address of the collector that will control this S-TAP, and to which this S-TAP will report and verify connectivity between the database server and the collector.
3. Copy the S-TAP installer to the local disk on the database server, typically to /tmp.
4. Extract the file with  

```
gzip -d <filename>.depot.gz
```
5. Enter the **swinstall** command as follows, supplying the selected file name (the appropriate native installer file) and your database server host name. This command starts an interactive program. Follow the prompts and use the appropriate controls to install the appropriate S-TAP installation program (.sh file), which is located in /var/spool/sw/var/tmp.  

```
swinstall -s /var/tmp/<filename>.depot @ ,hostname>:/var/spool/sw
```
6. Continue with [running the interactive installer](#) in the installation procedure, running the generated installation script rather than the default installation script for the operating system version.

## Remove HPUX S-TAP Using Native Installer

### Procedure

To remove HPUX S-TAP using the native installer, use the following command:

```
swremove @<hostname>:/var/spool/sw
```

## Linux-UNIX: Installing and uninstalling the S-TAP with Solaris native installer

### Before you begin

- Verify all [Linux-UNIX: S-TAP installation prerequisites](#).
- Obtain the correct native installer file (.pkg file), from either [Fix Central](#), or your Guardium representative.

### Procedure

1. Obtain the IP address of the database server on which you are installing S-TAP. If virtual IPs are used, note those as well (you will need to configure those later, when completing the configuration).
2. Identify the IP address of the collector that will control this S-TAP, and to which this S-TAP will report and verify connectivity between the database server and the collector.
3. Copy the S-TAP installer to the local disk on the database server, typically to /tmp.
4. Enter the **pkgadd** command to run the installer using the selected file:  

```
pkgadd -d <filename>.pkg
```

The shell installer is extracted under /usr/local/guardium
5. Continue with [running the interactive installer](#) of the installation procedure, running the extracted shell installer script rather than the default installation script for the operating system version.

## Remove AIX® S-TAP Using Native Installer

### Before you begin

- If A-TAP is active, de-activate it before uninstalling the S-TAP. See [Linux-UNIX: A-TAP activate, deactivate and DB stop, restart guidelines](#).

### Procedure

Enter to command:

## Linux-UNIX: S-TAP upgrade workflows per monitoring mechanism

The S-TAP upgrade workflow depends on your monitoring mechanism: K-TAP, exit library, A-TAP. Use these workflows together with the specific upgrade procedure.

### About this task

When upgrading S-TAP where K-TAP is also deployed, upgrade only the S-TAP in the global zone. (Without KTAP, there is no special procedure for upgrading S-TAP.)

- [Linux-UNIX: Upgrading S-TAP with databases that use A-TAP](#)  
Use this workflow when upgrading S-TAPs that use A-TAP monitoring.
- [Linux-UNIX: Upgrading S-TAP with databases that use an exit library](#)  
Understand the flow for upgrading an S-TAP whose databases use an exit library (Db2, Informix, Teradata).

### Related tasks

- [Linux-UNIX: Upgrading A-TAP in Zones and WPARs environment](#)

## Linux-UNIX: Upgrading S-TAP with databases that use A-TAP

Use this workflow when upgrading S-TAPs that use A-TAP monitoring.

### Procedure

1. Stop the databases.
2. De-instrument and de-activate all ATAPs (using guardctl).
3. Upgrade the S-TAP
4. Instrument and activate all A-TAPs.
5. Start the databases.

### Related reference

- [Linux-UNIX: guardctl utility commands for A-TAP](#)

## Linux-UNIX: Upgrading S-TAP with databases that use an exit library

Understand the flow for upgrading an S-TAP whose databases use an exit library (Db2, Informix, Teradata).

### About this task

If you are upgrading your S-TAP from v10.6.0.0 and later, all you need to do is to upgrade your S-TAP. The databases do not need to be stopped, and restart is not required. Database traffic continues to be monitored during the upgrade. After the upgrade the database continues to be fully monitored and fully operational, but using the previous version of the exit library. The next time the database is restarted, the newest version of exit library is automatically used. The restart can be performed at any time, even weeks later. If you have more than one database, or more than one instance of a database, they can be restarted individually; they do not need to be restarted at the same time. If there are any issues addressed in the new library that you are waiting for, however, you must restart the database.

If you are upgrading your S-TAP from pre-v10.6.0.0 to v10.6.0.0 and later, you must determine whether your exit library is copied or linked.

- If it is copied, then the library needs to be deleted. You'll create a linked library after upgrading the S-TAP.
- If it is linked, make sure it's linked to the library in the standard library paths. If not, you'll remove the link and create new links after you upgrade the S-TAP.

This procedure covers all of these scenarios.

### Procedure

1. Stop the database service.
  - Teradata
    - Enter:  

```
/etc/init.d/tpa stop
/etc/init.d/tgtw stop
```
    - Check that the Teradata database is stopped with your Teradata Administrator, or with the UNIX command:  

```
pdestate -a
```

The response should be:  

```
PDE state: DOWN/HARDSTOP
```

2. Verify if your exit library is copied or linked, and whether or not the link is correct. Depending on your database, these are the commands and expected responses if the library is linked to the standard library path:

Db2

```
ls -l $DB2_PATH/sqllib/security64/plugin/commexit/
lrwxrwxrwx 1 db2inst1 db2iadm1 34 Mar 13 18:24 libguard_db2_exit_64.so ->
/usr/lib64/libguard_db2_exit_64.so
```

Informix

```
ls -l $INFORMIXDIR/lib/libguard_informix_exit_64.so
lrwxrwxrwx 1 informix informix 39 May 22 18:31 libguard_informix_exit_64.so ->
/usr/lib64/libguard_informix_exit_64.so
```

Teradata

```
ls -l <Teradata_install_directory>/tdat/tgtw/site/
lrwxrwxrwx 1 teradata tdtrusted 39 Jun 25 13:51 libtgtwmonitoring.so ->
/usr/lib64/libguard_teradata_exit_64.so
```

If the library is linked to the standard library path, perform step [4](#).

If the response is anything else, perform steps [3](#), [4](#), and [5](#).

3. Remove the current link to libtgtwmonitoring.so:

Db2

Enter:

```
rm -rf $DB2_PATH/sqllib/security64/plugin/commexit/*
```

Informix

Enter:

```
rm -rf $INFORMIXDIR/lib/*
```

Teradata

a. Enter:

```
rm -rf <Teradata_install_directory>/tdat/tgtw/site/*
```

b. Verify the Link is removed by entering:

```
ls -ltr <teradata_install_directory>/tdat/tgtw/site/
```

The response should not include libtgtwmonitoring.so, indicating the link was successfully removed.

4. Upgrade the S-TAP. If the database has a link to the standard library path, the S-TAP automatically updates the link for the new (later) version.

5. Link libtgtwmonitoring.so to /usr/lib64/libguard. Execute the appropriate command for your database:

Db2

As Db2 OS user, create the linked library by running one of these commands, depending on the OS:

- ln -fs /usr/lib64/libguard\_db2\_exit\_64.so \$DB2\_PATH/sqllib/security64/plugin/commexit/libguard\_db2\_exit\_64.so
- ln -fs /usr/lib/64/libguard\_db2\_exit\_64.so \$DB2\_PATH/sqllib/security64/plugin/commexit/libguard\_db2\_exit\_64.so
- ln -fs /usr/lib/libguard\_db2\_exit\_64.so \$DB2\_PATH/sqllib/security64/plugin/commexit/libguard\_db2\_exit\_64.so

Informix

As Informix OS user, create the linked library by running one of these commands, depending on the OS:

- ln -fs /usr/lib64/libguard\_informix\_exit\_64.so \$INFORMIXDIR/lib/libguard\_informix\_exit\_64.so
- ln -fs /usr/lib/64/libguard\_informix\_exit\_64.so \$INFORMIXDIR/lib/libguard\_informix\_exit\_64.so
- ln -fs /usr/lib/libguard\_informix\_exit\_64.so \$INFORMIXDIR/lib/libguard\_informix\_exit\_64.so

Teradata

a. As Teradata OS user, create the linked library by running one of these commands, depending on the OS:

- ln -fs /usr/lib64/libguard\_teradata\_exit\_64.so /opt/teradata/tdat/tgtw/site/libtgtwmonitoring.so
- ln -fs /usr/lib/64/libguard\_teradata\_exit\_64.so /opt/teradata/tdat/tgtw/site/libtgtwmonitoring.so
- ln -fs /usr/lib/libguard\_teradata\_exit\_64.so /opt/teradata/tdat/tgtw/site/libtgtwmonitoring.so

b. Confirm the link was created by entering:

```
ls -l <Teradata_install_directory>/tdat/tgtw/site/
```

The response should be similar to:

```
lrwxrwxrwx 1 teradata tdtrusted 39 Jun 25 13:51 libtgtwmonitoring.so -> /usr/lib64/libguard_teradata_exit_64.so
```

6. Start the database service:

Teradata

a. Enter:

```
/etc/init.d/tpa start
/etc/init.d/tgtw start
```

b. Verify that the Teradata database is started with your Teradata Administrator, or with the UNIX command:

```
pdestate -a
```

The response should be:

```
PDE state is RUN/STARTED.
DBS state is 5: Logons are enabled - The system is quiescent
```

## Results

---

Your exit library will upgrade the next time you restart your database.

## Related tasks

---

- [Linux-UNIX: Configuring Exit libraries](#)
  - [Linux-UNIX: Upgrading an S-TAP agent with GIM Setup by Client](#)
  - [Linux-UNIX: Upgrading S-TAP using RPM](#)
  - [Linux-UNIX: Upgrading the S-TAP agent using the shell installer](#)
- 

## Linux-UNIX: Working with K-TAP

K-TAP is a kernel module that is installed into the database server operating system during S-TAP installation. After it is installed, it can be enabled or disabled with a configuration file setting. When enabled, it observes access to a database server by hooking the mechanisms used to communicate between the database client and the server. With K-TAP you do not need to change how database clients connect to the server.

Important: K-TAP does not support Ksplice or any other live kernel patching mechanism. To use K-TAP in your Linux environment, you must disable live kernel patching, including Ksplice extensions and similar mechanisms, such as Ubuntu Linux livepatch or SUSE Linux Live Patching.

Note: If K-TAP fails to load properly during installation, possibly caused by hardware or software compatibility, P-CAP is installed as the default collection mechanism. See [Linux-UNIX: Enable K-TAP after installation if P-CAP was installed by default](#).

- [Linux-UNIX: Preparing to install K-TAP](#)  
The S-TAP installation process checks the database kernel to determine whether a K-TAP has been created to work with that kernel. If not, the K-TAP Loader can create the K-TAP by compiling it, or by using the FlexLoad mechanism. For Linux databases, you can check in advance using the [Finding the correct K-TAP version for your Linux kernel](#) database, if there is a matching K-TAP.
- [Linux-UNIX: S-TAP compilation of K-TAP](#)  
There are hundreds of Linux distributions available, and the list is growing. This means that there might not be a K-TAP already available for your Linux distribution. If the correct K-TAP is not available, the S-TAP installation process can build it for you.
- [Linux-UNIX: Enrolling a K-TAP signing key](#)  
Use the following procedure to enroll the Guardium® signing key on any database server that requires secure boot and uses the K-TAP that is supplied by Guardium. The Guardium key must be enrolled on any servers before you install S-TAP.
- [Linux-UNIX: Signing and enrolling a locally built K-TAP](#)  
Use the following procedure to sign and enroll a signing key on any database server that requires secure boot and uses a locally built K-TAP. The Guardium key must be enrolled on the server before you install S-TAP.
- [Linux-UNIX: Copying a K-TAP module with GIM](#)  
If you build a custom K-TAP module for a Linux database server, you can use GIM to copy that module to other servers that are running the same Linux distribution. For example, you can build a K-TAP on a test system and then copy it to one or more production database servers after testing.
- [Linux-UNIX: Copying a K-TAP module from the command line](#)  
Use the command line to copy a new K-TAP module from one Linux database server to other database servers that run the same Linux distribution.
- [Linux-UNIX: Enable K-TAP after installation if P-CAP was installed by default](#)  
If, during the installation process, K-TAP fails to load properly, possibly caused by hardware or software incompatibility, P-CAP is installed as the default collection mechanism. To switch to K-TAP, after compatibility issues are resolved, follow these steps.
- [Linux-UNIX: Requesting a K-TAP module](#)  
Perform this procedure before upgrading your Linux operation system to determine if there is a matching K-TAP module for the new kernel level, and if not to request the K-TAP module from Technical Support.
- [Linux-UNIX: K-TAP FAQs](#)  
Find answers to commonly asked questions about K-TAP.

## Linux-UNIX: Preparing to install K-TAP

---

The S-TAP installation process checks the database kernel to determine whether a K-TAP has been created to work with that kernel. If not, the K-TAP Loader can create the K-TAP by compiling it, or by using the FlexLoad mechanism. For Linux databases, you can check in advance using the [Finding the correct K-TAP version for your Linux kernel](#) database, if there is a matching K-TAP.

This flow is relevant for S-TAP installation with both GIM and non-GIM.

FlexLoad mechanism guidelines:

- SUSE requires that the primary kernel version (for example, 4.12.14 of the version 4.12.14-23.1) matches and the vendor specific version falls within range of a release: the digits following 4.12.14 have to be higher than the existing module in the list.
  - All others require that the primary kernel version (X.Y.Z) matches in addition to the major vendor specific version number (A in X.Y.Z-A.B.C). The digits following X.Y.Z in the OS kernel version have to be higher than the module to be flex loaded. For example, kernel 3.10.0-514.6.1.el7.ppc64le would accept a flex match for a module built for 3.10.0-514.2.2.el7.ppc64le.
  - In all cases, the kernel module representing the most recent kernel that matches the rules, and also is older than the kernel version installed, is chosen. Module families also need to match, for example, el5, el6, el7, pae, x86\_64, and so on.
1. For Linux databases only: Check if your database operating system-kernel version has a K-TAP module match.
    - a. On your database, as user root, run the command: `uname -r` to output only the kernel version. The kernel version is similar to: 2.6.18-164.10.1.el5.
    - b. Open the [Finding the correct K-TAP version for your Linux kernel](#) database.
    - c. Paste in your kernel version, select your Guardium version and operating system, and click Search. The database filters to show the relevant K-TAP version. There are three possibilities:
      - The Match column displays either **Exact**. There is an exact match. You can proceed with the S-TAP installation.
      - The Match column displays either **Flex**. Enable the FlexLoad mechanism when installing S-TAP, (step 4), or have the S-TAP compile the K-TAP during installation (step 3).

- There is no match at all. In this case you can either have S-TAP compile the K-TAP, or you can order a custom build (step 6).
2. For non-Linux databases: Look at the list of supported kernels in the fix pack of the target S-TAP install version , for example Guardium\_10.6\_KTAP\_List.zip, from [Fix Central](#).
- If there is a match, You can proceed with the S-TAP installation.
  - If there is no match, you can either compile the K-TAP during S-TAP installation (step 3), you can try to Flex Load (step 4), or you can order a custom K-TAP ([Linux-UNIX: Requesting a K-TAP module](#)).
3. If K-TAP Loader did not find an exact match or a close match, AND if FlexLoad mechanism is OFF, AND if the database system has the required packages installed (see [Linux-UNIX: S-TAP compilation of K-TAP](#)), it attempts to build one to match your Linux kernel. All you need to build the K-TAP is the S-TAP installer.
4. If K-TAP Loader cannot find the correct kernel module, AND if FlexLoad mechanism is ON, K-TAP Loader finds the closest matching kernel module and loads it. The FlexLoad mechanism is controlled by:
- GIM installation: KTAP\_ALLOW\_MODULE\_COMBO
  - shell installation: --ktap\_allow\_module\_combo
  - RPM: --set-flexload
5. If you ordered a custom K-TAP build, after two weeks you'll have a custom modules-xxx.tgz file. You specify that file during the shell install with the --modules flag, or with the GIM \_ALLOW\_CUSTOMED\_BUNDLES flag when installing with GIM.
6. If K-TAP cannot load the kernel module by any of these three modes, it informs you with a "Failed to load" message. It either installs the S-TAP without the K-TAP (and with PCAP instead), or fails the S-TAP installation. If you reach this point, you'll need to order a custom K-TAP build.
7. If you have several systems running the same Linux distribution, you can build a K-TAP on one system and copy it to the others. For example, you might build a K-TAP on a test system and then copy it to one or more production database servers after testing. If you use GIM to install the S-TAP, GIM can automatically copy the bundle containing the new K-TAP to a Guardium® system from which you can distribute it to other database servers.

## Related tasks

---

- [Linux-UNIX: Requesting a K-TAP module](#)
- [Linux-UNIX: Copying a K-TAP module with GIM](#)
- [Linux-UNIX: Copying a K-TAP module from the command line](#)

## Related reference

---

- [Linux-UNIX: K-TAP parameters](#)

## Linux-UNIX: S-TAP compilation of K-TAP

---

There are hundreds of Linux distributions available, and the list is growing. This means that there might not be a K-TAP already available for your Linux distribution. If the correct K-TAP is not available, the S-TAP installation process can build it for you.

Most of the K-TAP code is independent of the kernel. The installer enables the code to interact with your kernel. This layer is delivered as proprietary source code. The installer builds the complete K-TAP by compiling this proprietary source code against your Linux kernel. This produces a K-TAP specific to your Linux distribution.

This process requires that the standard kernel development utilities, provided with Linux distribution, are present on the database server where the K-TAP is to be built. The development package must be an exact match for the kernel. The required packages are:

- RedHat based servers:
  - kernel-devel- `uname -r` for booted kernel
  - gcc compiler package
- Suse based servers:
  - kernel-devel or kernel-source(if available) for booted kernel
  - kernel-default-devel for booted kernel
  - gcc compiler package
- Ubuntu/Debian based servers:
  - linux-headers for booted kernel image
  - gcc compiler package

Important: Ensure that the server has the minimum required GNU Compiler Collection (GCC) version or a newer version installed, as supported by the kernel. When the installer attempts to build a K-TAP module, you see messages issued by guard-ktap-loader. These messages can include:

- It is attempting to build
- The build has completed
- The K-TAP has been loaded
- The build cannot be attempted because the kernel development package is not found
- [Linux-UNIX: Copying a K-TAP module from the command line](#)
- [Linux-UNIX: Copying a K-TAP module with GIM](#)

## Linux-UNIX: Enrolling a K-TAP signing key

---

Use the following procedure to enroll the Guardium® signing key on any database server that requires secure boot and uses the K-TAP that is supplied by Guardium. The Guardium key must be enrolled on any servers before you install S-TAP.

## Before you begin

---

Enrolling the key requires that you have root privileges and system console access. The modules are signed by IBM, but you need to enroll the Guardium signing key on to the secure boot-enabled system.

Use the following command to determine whether secure boot is enabled on the server:

```
mokutil --sb-state
```

Response,

- **Secure boot disabled** - The procedure is not needed.
- **Secure boot enabled** - Complete this procedure to enroll the Guardium key.

## About this task

You need to enroll the key the first time that you install a K-TAP with kernel signing. Subsequent upgrades use the same key.

## Procedure

1. Obtain the correct installer script from either [Fix Central](#) or from your Guardium representative, and extract guardium\_module\_signing.der from the compressed file (located under a folder named **Kernel\_Signing**).
2. Copy the file with Guardium signing key guardium\_module\_signing.der to a server where secure boot is enabled.  
Note: Check that the signing key file is correct for your server. For example, for SUSE 15, the key is called guardium\_module\_signing\_suse15.der.
3. On the server, log in as root and enter the following command to enroll the key:

```
mokutil --import guardium_module_signing.der
```

Note: Specify a password to enter when the system restarts. You are prompted for the password after the BIOS POST, but before the kernel starts (in the EFI shim).

4. Verify that you have access to the system console.
5. Restart the system when possible.
  - a. During the start-up process, press any key when the system returns the following prompt, Press any key to perform MOK management.
  - b. Under **Perform MOK Management**, select Enroll MOK.
  - c. Click View key to see the certificate details, and then press Enter (or choose Continue).
  - d. At the system prompt **Enroll the key(s) ?**, click Yes.
  - e. Enter the enrollment password (the password that you used with the **mokutil --import** command in step 3).
  - f. Select Reboot.

## What to do next

Enter the following command to confirm the key's presence in the system keyring.

```
cat /proc/keys | grep Guardium
```

Example output,

```
06dd7037 I----- 2 perm 1f010000 0 0 asymmetri IBM Guardium Secure Boot Signing:
d0609780bff59335919e575279c9b20b6728ca93: X509.RSA 6728ca93
```

## Linux-UNIX: Signing and enrolling a locally built K-TAP

Use the following procedure to sign and enroll a signing key on any database server that requires secure boot and uses a locally built K-TAP. The Guardium® key must be enrolled on the server before you install S-TAP.

## Before you begin

If your site uses secure boot, and you want to use a local K-TAP build, then you can use the **kernelModuleSigning.sh** script to sign the locally built K-TAP module before you install S-TAP and K-TAP. The **kernelModuleSigning.sh** script helps automate upgrading or installing a new K-TAP.

To check whether secure boot is enabled on the server, run the following command :

```
mokutil --sb-state
```

Response:

- **Secure boot disabled** - The procedure is not needed.
- **Secure boot enabled** - Complete this procedure to enroll the Guardium key.

Note: 12.0 and later **kernelModuleSigning.sh** is included as part of your S-TAP package starting with versions 12.0.

## Procedure

1. If your company already has a public/private signing key, use that signing key. If you do not already have a signing key, use the following example to generate one. Enter the following code.

```
cat <<EOF >signfile.config
[req]
distinguished_name = req_distinguished_name
x509_extensions = v3
string_mask = utf8only
prompt = no
[req_distinguished_name]
O =<Key - Example>
CN = Secure Boot Signing
emailAddress = <example@yourcompany.com>

[v3]
subjectKeyIdentifier = hash
```

```
authorityKeyIdentifier = keyid
basicConstraints = critical,CA:FALSE
keyUsage = digitalSignature
extendedKeyUsage = codeSigning
```

```
EOF
```

Note: Replace the **organization (O)** and **emailAddress** lines with your own information.

```
openssl req -config ./signfile.config -new -x509 -newkey rsa:4096 -nodes -days 3650 -outform DER -keyout signfile.priv -
out signfile.der

openssl x509 --inform der --in signfile.der --text --noout > signfile.crt
```

2. Use **mokutil** to enroll your new key in the secure boot cache on database server and follow the instructions in the script.

For example:

```
mokutil --import ./signfile.der
```

3. Verify that you have access to the system console.

4. Restart the system when possible.

- a. During the start-up process, press any key when the system returns the following prompt, Press any key to perform MOK management.

- b. Under **Perform MOK Management**, select Enroll MOK.

- c. Click View key to see the certificate details, and then press Enter (or choose Continue).

- d. At the system prompt **Enroll the key(s) ?**, click Yes.

- e. Enter the enrollment password (the password that you used with the **mokutil --import** command in step).

- f. Select Reboot.

5. Proceed with your standard shell or bundle S-TAP fresh installation. You might need to upgrade afterward. When the installation starts, an error that is similar to the following displays:

```
<13>Dec 5 16:25:37 guard_ktap_loader: Custom module ktap-112810-rhel-8-linux-x86_64-xCUSTOMxrh8u5x64t-4.18.0-
372.26.1.e18_6.x86_64-x86_64-SMP.ko built for kernel 4.18.0-372.26.1.e18_6.x86_64.

<13>Dec 5 16:25:46 guard_ktap_loader: Cannot install ktap at this time, please contact IBM.
Could not start KTAP

<13>Dec 5 16:25:46 guard_ktap_loader: ktap module is not loaded at this time.
```

6. Don't panic! Run the **kernelModuleSigning.sh** utility on the database server where the S-TAP is running. Follow the instructions that display on the screen to sign your locally built K-TAP module (**ktap\*xCUSTOM\*.ko**) with the public and private signing keys.

After signing the keys, the script walks you through the next steps to finish the installation.

## Results

Enter the following code to confirm that the key is available in the system keyring:

```
cat /proc/keys | grep -i <key_word_of_key>
```

A successful response is similar to the following example:

```
cat /proc/keys | grep -i 'Key-Example'
0c113cc5 I----- 1 perm 1f010000 0 0 asymmetric Key-Example: Secure Boot Signing:
6c0351ef68bb6fd1d24501d461008d9813b3ca: X509.rsa 8d13b3ca []
```

## Linux-UNIX: Copying a K-TAP module with GIM

If you build a custom K-TAP module for a Linux database server, you can use GIM to copy that module to other servers that are running the same Linux distribution. For example, you can build a K-TAP on a test system and then copy it to one or more production database servers after testing.

### Before you begin

- Verify that STAP\_UPLOAD\_FEATURE=1 on the database on which you are going to build the custom module. By default, the parameter STAP\_UPLOAD\_FEATURE is 1. The default enables automatic upload of the newly built K-TAP module to the Guardium® system that hosts the GIM server that manages the S-TAP bundle. This setting does not affect S-TAP diagnostic files. They are uploaded to the Guardium system that the S-TAP is registered with.
- Set GIM\_ALLOW\_CUSTOMED\_BUNDLES=1 on each DB server that you want to copy the K-TAP module to. For security reasons, this parameter must be set manually on each DB server. GIM\_ALLOW\_CUSTOMED\_BUNDLES=1 cannot be changed from 0 to 1 in the GUI or the API. Only the operating system admin can change the value from 0 to 1 after GIM is installed. This parameter can be set to either 1 or 0 when you use the configurator utility on the DB server. This functionality is checked during the K-TAP installation (on the DB server). It is not checked while you are assigning or scheduling a bundle installation or a parameter update (like all the other parameters are validated). (You can set GIM\_ALLOW\_CUSTOMED\_BUNDLES=0 from the Guardium system.)
- The GIM client is installed and points to the central manager.

Note: The S-TAP bundle is always visible in the GIM GUI. However, the S-TAP console displays only the S-TAP agent if **sqlguard\_tapip** (in **guard\_tap.ini**) points to the same IP that is listed in the GIM configuration 'gim\_url'.

If **sqlguard\_tapip** points to a different IP address, then the S-TAP agent does not display in the S-TAP console.

### About this task

The custom K-TAP module is built when you install the S-TAP on a Linux server for which no pre-built K-TAP exists for the current kernel, but only if the kernel-devel package is installed. The S-TAP bundle is visible in the GIM GUI, regardless of which appliance the S-TAP agent points to. Uploading this module initiates creation of a custom S-TAP bundle. Bundle numbers have an appended suffix that starts with \_800 and increases by 1 with each additional bundle, for example BUNDLE\_STAP (10.1.4\_r102728\_800).

## Procedure

---

1. Use GIM to install the S-TAP on the Linux database server. Set the parameter STAP\_SQLGUARD\_IP=IP of the MU. The installer determines that a custom K-TAP module is required and builds it.
2. Transfer this bundle to other managed units:
  - a. On the central manager, go to **Manage > Central Management > Central Management**
  - b. In the table of managed units, select the managed units that you want to copy the bundle to.
  - c. Click Distribute GIM bundles.
3. Use [Set up by Client](#) to install the bundle on the managed units.
  - [Linux-UNIX: Copying a K-TAP module from the command line](#)

## Linux-UNIX: Copying a K-TAP module from the command line

---

Use the command line to copy a new K-TAP module from one Linux database server to other database servers that run the same Linux distribution.

### Before you begin

---

Use this procedure after you have built and tested a K-TAP module on a Linux database server.

### Procedure

---

1. Log in to the database server with the tested K-TAP module.
2. Change directory to /usr/local/guardium/guard\_stap/ktap/current/ and run **./guard\_ktap\_append\_modules** to add the locally built modules to modules.tgz.
3. Repeat step 1.
4. Copy the updated modules.tgz file to the target database server.
5. Log in to the target database server and change the directory to /usr/local/guardium/guard\_stap/ktap/current/.
6. Resolve any issues with the K-TAP, such as submitting a module request to IBM or installing kernel development packages.

Note: If you installed a GIM S-TAP bundle, set export GIM\_CONTEXT=Y. For example:

```
export GIM_CONTEXT=Y
```

7. Run the **guard\_ktap\_loader retry** script from the ktap directory. For example:

- shell/RPM installation:

```
guardium/guard_stap/ktap/current/guard_ktap_loader retry
```

GIM installation:

```
export GIM_CONTEXT=Y; modules/KTAP/current/guard_ktap_loader retry
```

8. Restart the S-TAP to connect it to the new K-TAP module.

### Results

---

The custom K-TAP module is ready to use on the target system. Repeat this procedure for each matching Linux system to which you want to deploy the K-TAP module.

- [Linux-UNIX: Copying a K-TAP module with GIM](#)
- [Linux-UNIX: K-TAP parameters](#)

## Linux-UNIX: Enable K-TAP after installation if P-CAP was installed by default

---

If, during the installation process, K-TAP fails to load properly, possibly caused by hardware or software incompatibility, P-CAP is installed as the default collection mechanism. To switch to K-TAP, after compatibility issues are resolved, follow these steps.

### Procedure

---

1. Resolve any issues with the K-TAP, such as submitting a module request to IBM or installing kernel development packages.

Note: If you installed a GIM S-TAP bundle, set export GIM\_CONTEXT=Y. For example:

```
export GIM_CONTEXT=Y
```

2. Run the script **guard\_ktap\_loader retry** from the ktap directory:

- shell/RPM installation: guardium/guard\_stap/ktap/current
- GIM installation: modules/KTAP/current

If K-TAP loads successfully, the guard\_tap.ini parameter ktap\_installed is automatically set to 1 (yes).

## Linux-UNIX: Requesting a K-TAP module

---

Perform this procedure before upgrading your Linux operation system to determine if there is a matching K-TAP module for the new kernel level, and if not to request the K-TAP module from Technical Support.

## Procedure

1. Access [Fix Central](#) and select the product and version per your need, and click Continue.

Type the product name to access a list of product choices.

When using the keyboard to navigate the page, use the **Tab** or **down arrow** key to move between fields.

Product selector\*

IBM Security Guardium

Installed Version\*

10.0

Platform\*

All

**Continue**

2. Enter `ktap` in the text field, and click Continue.

### Identify fixes

IBM Security, IBM Security Guardium (All releases, All platforms)

Search for fixes for your specific product, type, and platform or search for

- Browse for fixes** Browse for all fixes for your specific product, type, and platform.
- APAR or SPR** Search for fixes by entering one or more APAR or SPR numbers.
- Individual fix IDs** Search for updates by entering one or more individual fix IDs (e.g., 5.2.0-15411\_linux\_32-64).
- Text** Search for fixes containing all the words you enter in the text field.
- ktap

**Continue**

**Back**

The K-TAP Bundle results appear.

3. Select fix pack: `KTAP_List_of_Modules_v10`, and click Continue.
4. Follow the instructions to acquire the file. For example, to download using HTTPS:

### Download files using HTTPS

IBM Security, IBM Security Guardium (10.0, All platforms)

[Subscribe to support notifications](#)

#### Download files using your web browser

Click the download link next to each file to download it.

Order number: 324749047

Total size: 20.67 KB

[Show normalized list](#) | [Hide normalized list](#)

#### fix pack: KTAP\_List\_of\_Modules\_v10

[KTAP\\_List\\_of\\_Modules\\_v10 \(All v10.x\)](#)

The following files implement this fix.

[!\[\]\(963e703aaa46d580ef5bd543d82c5c3f\_img.jpg\) KTAP\\_List\\_of\\_Modules\\_v10.zip \(20.67 KB\)](#)

5. Save the zip file, and open it to verify if your OS kernel is supported by the latest K-TAP module release related to your version.

| The FixCentral entry corresponding to this file is<br>SUPPORTED OS KERNEL LEVEL (uname -r) | <a href="http://www.ibm.com/support/fixcentral/">http://www.ibm.com/support/fixcentral/</a><br>KTAP MODULE |
|--------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| #####platform=x86_64                                                                       | #####platform=x86_64                                                                                       |
| 2.6.18-128.1.10.el5                                                                        | 2.6.18-128.1.10.el5-x86_64-SMP.ko                                                                          |
| 2.6.18-128.1.10.el5xen                                                                     | 2.6.18-128.1.10.el5xen-x86_64-SMP.ko                                                                       |
| 2.6.18-128.1.14.el5                                                                        | 2.6.18-128.1.14.el5-x86_64-SMP.ko                                                                          |
| 2.6.18-128.1.16.0.1.el5                                                                    | 2.6.18-128.1.16.0.1.el5-x86_64-SMP.ko                                                                      |
| 2.6.18-128.1.16.el5                                                                        | 2.6.18-128.1.16.el5-x86_64-SMP.ko                                                                          |
| 2.6.18-128.1.1.el5                                                                         | 2.6.18-128.1.1.el5-x86_64-SMP.ko                                                                           |
| 2.6.18-128.1.6.0.1.el5                                                                     | 2.6.18-128.1.6.0.1.el5-x86_64-SMP.ko                                                                       |
| 2.6.18-128.1.6.el5                                                                         | 2.6.18-128.1.6.el5-x86_64-SMP.ko                                                                           |

6. If your kernel is not listed or not listed in the K-TAP list, open a Support Case: <https://www.ibm.com/mysupport/s/createrecord/NewCase>.

For each database server system you need the KTAP module for, you must provide these details:

- Kernel version (output of `uname -a`)
- Operating System version (output of `cat /etc/redhat-release` or, depending on the release `ls /etc/*release*` and then cat the output, or `cat /etc/issue`)
- CPU Info (output of `cat /proc/cpuinfo`)
- Database type and version
- Which version of S-TAP the K-TAP module needs to be compiled for

It typically takes up to 14 days to fulfill a new K-TAP module request. Guardium informs the customer when the new K-TAP module is available, ready to download.

## Linux-UNIX: K-TAP FAQs

Find answers to commonly asked questions about K-TAP.

Does K-TAP support Ksplice (or other live patching mechanisms)?

K-TAP does not support Ksplice or any other live kernel patching mechanism. To use K-TAP in your Linux environment, you must disable live kernel patching, including Ksplice extensions and similar mechanisms, such as Ubuntu Linux livepatch or SUSE Linux Live Patching.

Can one database server be used to build different custom K-TAP versions?

Yes. The module is created for the currently installed kernel on the server, so you must set the correct kernel and restart the server.

Do you need to regenerate and reinstall the custom K-TAP each time that the server receives a new kernel?

Yes.

What happens if the K-TAP is not up to date?

If the KTAP does not match the running kernel, it does not load.

Does a custom K-TAP need to have the same version as the S-TAP, or can a Guardium system have K-TAP and S-TAP that are running different versions?

K-TAPs and S-TAPs must run the same version.

When you install K-TAP by using the Flex method, Guardium determines which precompiled K-TAP is the most suitable for the installation. How is this procedure performed by Guardium?

See [Linux-UNIX: S-TAP compilation of K-TAP](#).

## Linux-UNIX: Special environments configuration

Use these procedures for as relevant for systems with Zones, RAC, WPAR, clusters.

- [Linux-UNIX: Solaris Zones configuration](#)  
Install and configure S-TAP in the Solaris global Zones (kernel zones). Non-global zones (local zones) share the resource with global zone.
- [Linux-UNIX: Oracle RAC S-TAP configuration](#)  
Oracle RAC (Real Application Clusters) allows multiple computers to run Oracle RDBMS software simultaneously while accessing a single database, thus providing clustering.
- [Linux-UNIX: Configure S-TAP for Db2 WPAR](#)  
Learn to configure S-TAP for Db2 WPAR
- [Linux-UNIX: Configure S-TAP for SELinux](#)  
Learn to configure S-TAP for Red Hat Security Enhanced Linux (SELinux).
- [Linux-UNIX: Activating and deactivating A-TAP on all nodes of a Db2 Cluster](#)  
Learn how to activate and deactivate A-TAP on the nodes of a Db2 cluster that share a Db2 cluster.
- [Linux-UNIX: Configure delayed cluster disk mounting](#)  
Configure S-TAP for delayed loading for Oracle, Informix® and DB2® database servers only.

## Linux-UNIX: Solaris Zones configuration

Install and configure S-TAP in the Solaris global Zones (kernel zones). Non-global zones (local zones) share the resource with global zone.

### About this task

This procedure covers both Solaris global Zones (kernel zones) and Non-global zones (local zones).

Solaris versions 10 and later implement virtualized operating environments called Zones. Each zone is self-contained and has its own hostname, IP address, storage, and process space. Processes running in one zone are disassociated from the other zones. There is an over-arching zone called the global Zone and every other zone is called a non-global or local zone.

S-TAP requires special configuration when it's installed in a zoned Solaris operating environment, since K-TAP, a kernel module, has to be installed in the global Zone, and it is shared between the local zones. This specific requirements are:

- S-TAP requires the **IP address of the database server host to which it connects**.

By default, S-TAP connects to the loopback address 127.0.0.1. This loopback address refers to the "local host", which is the global zone. Instead, obtain the IP address of the non-global zone using **ifconfig -a**. For example, in the zone dbserver01:

```
#ifconfig -a
....
....
*hme0:1: flags=1000843 mtu 1500 index 2
zone dbserver01inet 192.168.1.201 netmask ffffff00 broadcast 192.168.1.255*
....
....
```

The IP address of the zone "dbserver01" is 192.168.1.201. S-TAP must connect to this IP address rather than 127.0.0.1, in order to intercept database traffic to and from the zone dbserver01. Assuming that dbserver01 is DB\_0 is the guard\_tap.ini file, you would change:

```
[DB_0]
connect_to_ip=127.0.0.1

to

[DB_0]
connect_to_ip=192.168.1.201
```

You must edit the file guard\_tap.ini itself. You cannot update this configuration in the GUI.

- S-TAP requires the **path of the database server executable**.

Each zone is a self-contained operating environment. The path inside a particular zone is specific to that zone. For example, /opt/IBM/informix/11.70.UC3 can exist in each zone and yet each zone has a unique path.

S-TAP is installed in the global zone, therefore the database executable in the non-global zone must be accessible from the global zone. If the file system in the non-global zone is externally mounted via mechanisms like NFS, it is important that the mounted location has the required permission to be accessed from the global zone. Otherwise, the S-TAP cannot access the database executable: the S-TAP status is initially green in the collector GUI, but then turns red and stays red.

Since each non-global zone is a virtualized environment, paths inside a non-global zone are accessible from the global zone via a zone path prefix, which is the local zone. The syntax for the path to a particular zone is: <localzone>/root/<database server installation location>. Use the Solaris command **zoneadm** to obtain the prefixes for the various zones. For example, from the global zone:

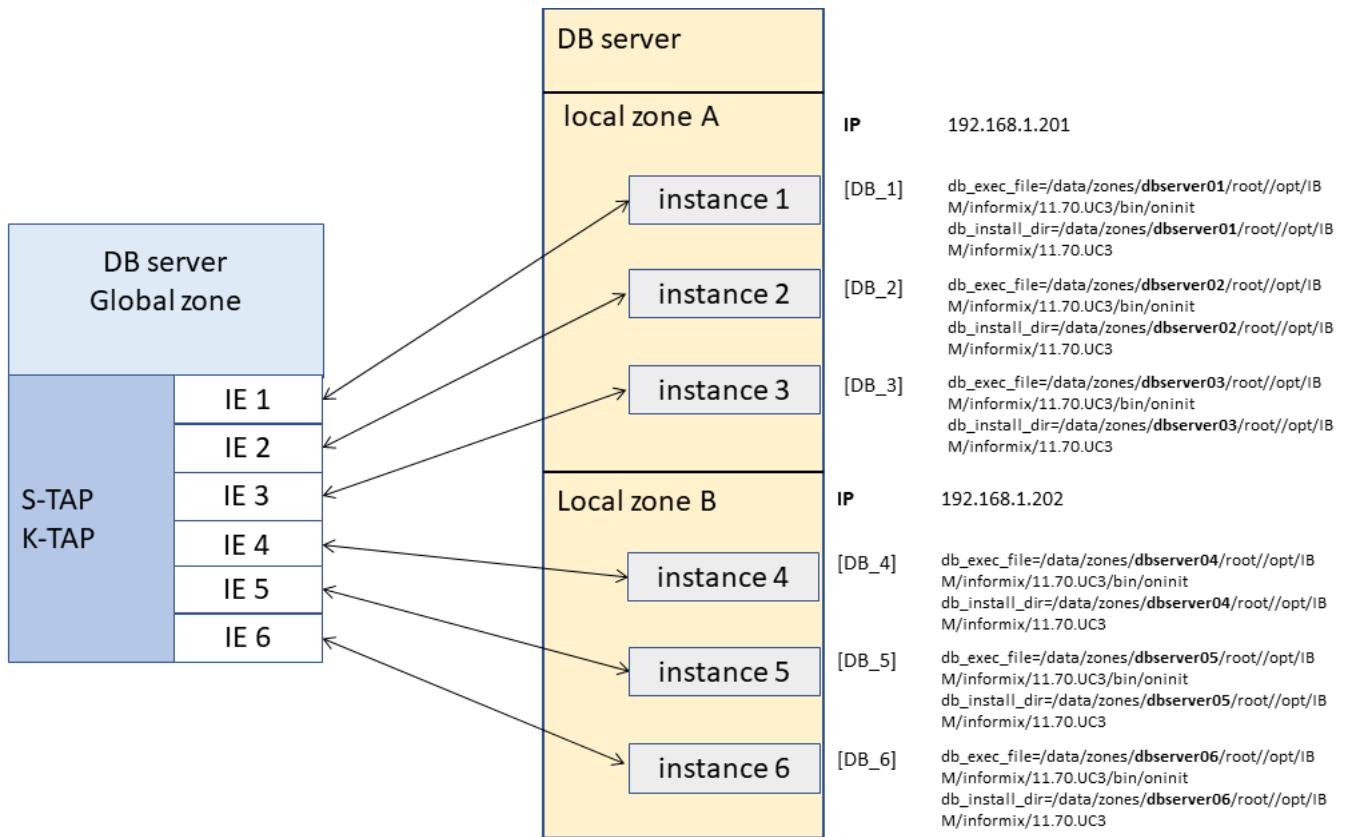
```
#zoneadm list -cv
ID NAME STATUS PATH
0 global running /
2 dbserver01 running /data/zones/dbserver01
3 dbserver02 running /data/zones/dbserver02
```

In this example output, there are two non-global zones: dbserver01 and dbserver02. The file structure inside each zone can be accessed from the global zone via /data/zones/dbserver01 and /data/zones/dbserver02 for the zones dbserver01 and dbserver02 respectively. Assuming that the database server is installed in /opt/IBM/informix/11.70.UC3 in the zone dbserver01, then the full path to that directory from the global zone would be:

/data/zones/dbserver01/root/opt/IBM/informix/11.70.UC3

When specifying the path to the database server executable and the install path to S-TAP, you must use this full zone relative path from the global zone. Using the IP address, the database server executable, and installation path, the guard\_tap.ini looks like:

```
[DB_1]
connect_to_ip=192.168.1.201
...
...
Path to the database server executable
db_exec_file=/data/zones/dbserver01/root//opt/IBM/informix/11.70.UC3/bin/oninit
Path to the database server installation
db_install_dir=/data/zones/dbserver01/root//opt/IBM/informix/11.70.UC3
...
```



**Multiple zones:** To monitor multiple non-global zones, create a DB section for each zone in the guard\_tap.ini file. To monitor dbserver02, add another section that includes:

```
[DB_2]
connect_to_ip=192.168.1.202
...
#
Path to the database server executable
db_exec_file=/data/zones/dbserver02/root//opt/IBM/informix/11.70.UC3/bin/oninit
Path to the database server installation
db_install_dir=/data/zones/dbserver02/root//opt/IBM/informix/11.70.UC3
...
...
```

## Procedure

1. Install S-TAP on the master zone (global zone) or kernel zone regardless of the zone in which the database runs, since the local zones share information from the master/kernel zone.
  2. Manually set S-TAP parameter connect\_to\_ip in the guard\_tap.ini file to the IP address of the non-global zone.
  3. When configuring the Inspection Engine, use the global/kernel zone values for the db\_install\_dir path and db\_exec\_file. These are the GUI parameters DB Install Dir, and Process Name, respectively. (From the global/kernel zone, S-TAP monitors access to databases in all zones.)
  4. Add the IP addresses of all zones that you want to monitor to the alternate\_ips parameter in the guard\_tap.ini file on the Solaris database server or use the S-TAP Control page to configure Alternate IPs.
- Typical parameter configuration:
- db\_exec\_file=/home/oracle18/app/oracle/product/18.0.0.0/dbhome\_1/bin/oracle (the full path to oracle executable)
  - db\_install\_dir=/home/oracle18/

## Results

- K-TAP is not loaded in the local zone as it is only loaded on the global zone. It is visible on the local zones.
- S-TAP does not run in the local zones.

## Related tasks

- [Linux-UNIX: Installing and activating A-TAP in Solaris zones](#)

## Linux-UNIX: Oracle RAC S-TAP configuration

Oracle RAC (Real Application Clusters) allows multiple computers to run Oracle RDBMS software simultaneously while accessing a single database, thus providing clustering.

## About this task

---

In a non-RAC Oracle database, a single instance accesses a single database. The database consists of a collection of data files, control files, and redo logs located on disk. The instance comprises the collection of Oracle-related memory and operating system processes that run on a computer system.

In an Oracle RAC environment, two or more computers (each with an Oracle RDBMS instance) concurrently access a single database. This allows an application or user to connect to either computer and have access to a single coordinated set of data.

## Procedure

---

1. Install S-TAP on all nodes. In case GIM is used, install the GIM client on all nodes, then install the bundle S-TAP on all nodes.

2. Configure the S-TAP parameters. All of the parameters can be configured through the GIM UI.

- STAP\_TAP\_IP: public IP configured for the node
- STAP\_ALTERNATE\_IPS: comma separated list of VIPs (virtual IPs) configured for the node, and the scan listener

Tip: Use this command to retrieve the value for virtual hostnames to put in STAP\_ALTERNATE\_IPS:

```
su - grid -c 'cat $ORACLE_HOME/network/admin/*.ora' |grep -i host
```

For example:

```
[root@racvm121 ~]# su - grid -c 'cat $ORACLE_HOME/network/admin/*.ora' |grep -i host
LISTENER_RACVM121=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP) (HOST=<hostname>) (PORT=1521)) (ADDRESS=(PROTOCOL=TCP) (
```

- Configure S-TAP inspection engine parameter: unix\_domain\_socket\_marker=<key>, where <key> value can be found in listener.ora in the IPC protocol definition

Tip: Command to retrieve value for unix\_domain\_socket\_marker:

```
su - grid -c 'cat $ORACLE_HOME/network/admin/*.ora' |grep -i KEY
```

- Example: If the following is a description in the listener.ora

```
LISTENER=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC) (KEY=ORCL)))
```

then

```
unix_domain_socket_marker=ORCL
```

- Example: If there is more than one IPC line in listener.ora, use a common denominator of all the keys:

```
su - grid -c 'cat $ORACLE_HOME/network/admin/*.ora' |grep -i KEY
LISTENER=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC) (KEY=LISTENER)))
LISTENER_SCAN1=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC) (KEY=LISTENER_SCAN1)))
LISTENER_SCAN2=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC) (KEY=LISTENER_SCAN2)))
LISTENER_SCAN3=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=IPC) (KEY=LISTENER_SCAN3)))
```

Guardium uses a string search in the path. In this case LISTENER works for all four and should be used: unix\_domain\_socket\_marker=LISTENER

- Example: If there is no common denominator, create additional inspection engines with unix\_domain\_socket\_marker corresponding to the specific IPC key(s). For example the guard\_tap.ini may look similar to this example in the end:

```
[DB_0]
...
unix_domain_socket_marker=EXTPROC1522
...
[DB_1]
...
unix_domain_socket_marker=LISTENER
```

3. If the Oracle database is encrypted (ASO/SSL), activate A-TAP on all nodes (active and standby). This example shows an Oracle setup with two users: grid and oracle.

- a. Authorize users grid and oracle.

- b. Stop the instance on the node that is part of RAC environment using the grid environment by entering the command:

```
srvctl stop instance -db database_name -node node_name -force
```

- c. Verify that the instance on the node is stopped by entering the command from the grid environment:

```
srvctl status instance -db database_name -node node_name
```

- d. Configure A-TAP by entering the command:

```
/usr/local/guardium/guard_stap/guardctl --db-user=oracle --db-type=oracle --db-instance=oracle --db-home=$ORACLE_HOME
--db-version=18.0 store-conf
```

- e. Activate A-TAP by entering the command:

```
/usr/local/guardium/guard_stap/guardctl --db-instance=oracle activate
```

- f. Restart the instance on the node that is part of RAC environment using the grid environment by entering the command:

```
srvctl start instance -db database_name -node node_name
```

- g. Repeat steps [3.a](#) through [3.f](#) on all nodes of the RAC environment.

## Related reference

---

- [Linux-UNIX: guardctl utility commands for A-TAP](#)
- [Linux-UNIX: Database-specific guardctl parameters](#)

# Linux-UNIX: Configure S-TAP for Db2 WPAR

Learn to configure S-TAP for Db2 WPAR

## About this task

There are two methods of determining the shmem parameters:

- If your output to `db2 get dbm cfg | grep ASLHEAPSZ` is in English, use the script `find_db2_shmem_parameters.sh` ([1](#)). Its output lists the Db2 shared memory parameters defined in the Inspection Engines. You can run it from any directory. It requires the db2 instance name as parameter.
- If your output to `db2 get dbm cfg | grep ASLHEAPSZ` is not in English, compute the client I/O area offset (step [2](#)), then find the Db2 shared memory size (step [3](#)).

When `ktap_fast_shmem` set to 1, if there are multiple Db2 instances that are configured for a single WPAR in `guard_tap.ini` file and they have the same `db2_shmem_size`, then the `db2_fix_pack_adjustment` and `db2_shmem_client_position` are taken from the first Db2 section for that WPAR. So in cases where there are multiple Db2 instances running on the WPAR:

- If all Db2 instances have the same `db2_shmem_size`, `db2_fix_pack_adjustment`, and `db2_shmem_client_position`, the packets from all instances are collected even if only one instance is configured.
- If all Db2 instances have the same `db2_shmem_size`, but different `db2_fix_pack_adjustment` or `db2_shmem_client_position`, then only packets from the first configured Db2 instance are collected.

## Procedure

1. Run the script `find_db2_shmem_parameters.sh` from any directory, using the syntax: `find_db2_shmem_parameters.sh <instance name>`. Its output lists the Db2 shared memory parameters defined in the Inspection Engines.
2. (Perform only if output to `db2 get dbm cfg | grep ASLHEAPSZ` is not in English). Compute the client I/O area offset (`db2_shmem_client_position`).
  - a. Open a new bash shell as the db2 instance user.
  - b. Run the `ps -x` command to verify that the db2bp command processor is not currently running for this shell. You should not see a command called db2bp running. If it is running, either kill it or run a new shell.
  - c. Run the following:

```
db2 get database manager configuration | awk '/ASLHEAPSZ/{print $9 * 4096}'
```

The output is the required value for `db2_shmem_client_position`

3. (Perform only if output to `db2 get dbm cfg | grep ASLHEAPSZ` is not in English). To find the Db2 shared memory segment size (`db2_shmem_size`), perform one of:
  - This method gives the most accurate results.
    - Start a Db2 shared memory connection and keep it open.
    - Run this command to get the process ID for db2sysc: `ps -efaf | grep db2sysc`. The output looks like:

```
db2inst1 5309370 5505772 0 Nov 11 - 1232:12 db2sysc 0
```

In this example, the process ID is 5309370.

- Run this command to retrieve information about shared-memory processes: `ipcs -ma`. The output looks like:

```
IPC status from /dev/mem as of Wed Nov 20 13:21:45 CST 2013
T ID KEY MODE OWNER GROUP CREATOR CGROUP NATTCH SEGSZ CPID
m 2097152 0xffffffff D-rw----- pconsole system pconsole system 1 536870912 4522088
m 1 0x78000015 --rw-rw-rw- root system root system 3 16777216 3605314
m 2 0x78000016 --rw-rw-rw- root system root system 3 268435456 3605314
m 219152387 0xffffffff D-rw----- root system root system 1 536870912 5243842
m 1048580 0x61013002 --rw----- pconsole system pconsole system 1 10485760 4522088
m 10485765 0xd9fd8a61 --rw----- db2inst1 db2iadml db2inst1 db2iadml 5 47644672 5571082
m 9437190 0xd9fd8a74 --rw-rw-rw- db2inst1 db2iadml db2inst1 db2iadml 9 140852104 5571082
m 9437191 0xe52594858 --rw-rw--- oracle dba oracle dba 40 53687107584 3801352
m 3145736 0x52594801 --rw-rw--- root informix root informix 13 223019008 5702650
m 3145737 0xd9fd8b68 --rw-rw--- db2inst1 db2iadml db2inst1 db2iadml 1 58720256 6619354
m 3145738 0xffffffff D--rw----- db2fenc1 db2fadml db2inst1 db2iadml 7 268435456 5505772
m 11 0x52594802 --rw-rw--- root informix root informix 13 33439744 5702650
m 12 0x52594803 --rw-rw-rw- root informix root informix 13 573440 5702650
m 13 0xf2033f7e --rw----- sybase15 sybase sybase15 sybase 1 115564544 5178168
m 409993231 0x52594804 --rw-rw--- informix informix informix informix 13 8388608 5702650
m 763363344 0xffffffff D--rw----- db2inst1 db2iadml db2inst1 db2iadml 1 268435456 5309370
m 125829140 0xffffffff D--rw----- db2inst1 db2iadml db2inst1 db2iadml 2 131072 5309370
m 201326613 0xffffffff D--rw----- db2inst1 db2iadml db2inst1 db2iadml 1 163905536 5309370
m 103750230 0xffffffff D--rw----- db2inst1 db2iadml db2inst1 db2iadml 1 134217280 5309370
```

The output contains several columns beyond those shown here, but they do not affect this procedure. Find the line that contains the process ID that was identified in step [3.b](#) and also has a value of 2 under NATTCH. The Db2 shared-memory segment size is the value in the SEGSZ column. In this example, it is 131072.

- Tip: if the list returned in step [3.c](#) is too long, you can filter it by using the process ID. In this case, you would enter `ipcs -ma | grep 5309370`. The results do not contain the column headers, but you can look at the previous results to see the column headers and identify the correct line and column. In this example, it is the last line.

```
m 131072014 0xffffffff D--rw----- db2inst1 db2iadml db2inst1 db2iadml 1 1342177280 5309370
m 763363344 0xffffffff D--rw----- db2inst1 db2iadml db2inst1 db2iadml 1 268435456 5309370
m 227541013 0xffffffff D--rw----- db2inst1 db2iadml db2inst1 db2iadml 1 163905536 5309370
m 106353238 0xffffffff D--rw----- db2inst1 db2iadml db2inst1 db2iadml 2 131072 5309370
```

- Alternatively, use this method, which is easier but less accurate:  
ATAP and KTAP rely on the size for identification of the Application/Agent shared memory segments. These segments are then tapped for C2S and S2C packets. The segments are equal to the sum of the ASLHEAPSZ and RQRIOLBK parameters. DB2® allocates much larger segments. In most cases, the size is

equal to (ASLHEAPSZ + 1) \* 2 pages, or (ASLHEAPSZ + 1) \* 8192 bytes. Exact size can be determined by observation of the shared memory segments in the system before and after new Db2 local connection is created. Use this sequence of commands to determine the shared memory segment size. ipcs command parameters and output format differ from platform to platform. The following script is based on the AIX® version.

```
ipcs -ma | sort -n -2 +3 > /tmp/before.txt
db2 connect to <some_existing_database>ipcs -ma | sort -n -2 +3 > /tmp/after.txt
db2 terminate
diff /tmp/before.txt /tmp/after.txt | awk '{if ($10 == 2) print $11}'
```

4. Set these parameters in order to capture the Db2 shared memory traffic.

Table 1. Db2 Parameters

| Parameter                      | STAP Name                 | ATAP Name         |
|--------------------------------|---------------------------|-------------------|
| Packet header size             | db2_fixed_pack_adjustment | db2_header_offset |
| Client I/O area offset         | db2_shmem_client_position | db2_c2soffset     |
| Db2 shared memory segment size | db2_shmem_size            | db2_shmsize       |

## Linux-UNIX: Configure S-TAP for SELinux

Learn to configure S-TAP for Red Hat Security Enhanced Linux (SELinux).

### About this task

Installing aGuardium®S-TAP with SELinux requires a few extra installation steps.

Note: Make sure that your S-TAP version matches the version of the Guardium appliance.

### Procedure

1. Install the S-TAP, using one of the methods described in [Linux-UNIX: Install S-TAP agents installation flow](#).

2. After you install the S-TAP, log into the Guardium server as root run the following commands.

Set the *enforce* environment variable to 0 and open the *guard\_tap.ini* file:

```
[root@mycompany guard_stap]# setenforce 0
[root@mycompany guard_stap]# ps -ef|grep stap
root 9955 1 0 10:32 ? 00:00:00 /guardium/guardium/guard_stap/guard_stap
/guardium/guardium/guard_stap/guard_tap.ini
root 10038 1889 0 10:32 pts/0 00:00:00 grep --color=auto stap
```

3. Run the following commands to enable required Guardium policies:

```
[root@mycompany guard_stap]# sealert -a /var/log/audit/audit.log
[root@mycompany guard_stap]#ausearch -c 'guard_discovery' --raw | audit2allow -M my-guarddiscovery
[root@mycompany guard_stap]# semodule -i my-guarddiscovery.pp

[root@mycompany guard_stap]# ausearch -c 'guard_stap' --raw | audit2allow -M my-guardstap
[root@mycompany guard_stap]# semodule -i my-guardstap.pp

[root@mycompany guard_stap]# ausearch -c 'guard_ktap_load' --raw | audit2allow -M my-guardktapload
[root@mycompany guard_stap]# semodule -i my-guardktapload.pp
```

4. Set the *enforce* environment variable back to 1.

```
[root@mycompany guard_stap]# setenforce 1
```

5. Restart the S-TAP.

## Linux-UNIX: Activating and deactivating A-TAP on all nodes of a Db2 Cluster

Learn how to activate and deactivate A-TAP on the nodes of a Db2 cluster that share a Db2 cluster.

### About this task

Activate A-TAP to capture encrypted traffic and shared memory traffic in Linux.

### Procedure

1. Authorize Db2 user on all nodes by running the following command.

```
<guardium_base>/xxx/guardctl authorize-user <user-name>
```

In the following example, user *db2inst1* is authorized.

```
/usr/local/guardium/bin/guardctl authorize-user db2inst1
/usr/local/guardium/bin/guardctl is_userAuthorized db2inst1
```

2. Configure A-TAP on all nodes.

3. Shut down the active node (node 1).

4. Activate A-TAP on node 1 by running the following command.

```
<guardium_base>/xxx/guardctl db_instance=<instance> activate
```

In the following example, `db2inst1` is node 1 and it is activated.

```
/usr/local/guardium/guard_stap/guardctl db_instance=db2inst1 activate
/usr/local/guardium/guard_stap/guardctl list-active
```

5. After you activate A-TAP on the original db2 server on node 1, do the following tasks:

- Restore the original Db2 server on node 1 so that other nodes can activate A-TAP. (All nodes share the executable).
- In the Db2 adm directory, copy `db2sysc-guard-original` over `db2sysc` (make a copy of each first and set them aside) by running the following command.

```
> cp db2sysc-guard-original db2sysc
```

6. Delete `db2sysc-guard-original` (otherwise, it fails activation on node 2) by running the following command.

```
rm -rf db2sysc-guard-original
```

7. Move cluster resources to node 2 by running the following command.

```
pcs resource move resource_id <destination node>
```

8. Activate A-TAP on node 2. This step creates the libraries on node 2 and replaces `db2sysc-guard-original`.

The following examples show the status for each node:

Node 1:

```
/usr/local/guardium/guard_stap/guardctl list-active
db2inst1
```

Node 2:

```
/usr/local/guardium/guard_stap/guardctl list-active
db2inst1
```

## Deactivating A-TAP on the nodes of a Db2 Cluster

Deactivate A-TAP on the active and passive nodes of a Db2 cluster when you upgrade the database or an S-TAP agent.

### Procedure

- Log in to the active node (node1).
- Shutdown the Db2 instance.
- Deactivate A-TAP on node 1.

For example:

```
/usr/local/guardium/guard_stap/guardctl db_instance=db2inst1 deactivate
```

- Deactivate A-TAP on all passive nodes by using the `force` option.

For example:

```
/usr/local/guardium/guard_stap/guardctl db_instance=db2inst1 --force-action=yes deactivate
```

## Related concepts

- [Linux-UNIX: A-TAP management](#)

## Linux-UNIX: Configure delayed cluster disk mounting

Configure S-TAP for delayed loading for Oracle, Informix® and DB2® database servers only.

When the S-TAP starts it must have access to the database home. If your environment uses a clustering scheme in which multiple nodes share a single disk that is mounted on the active node, but not on the passive node, the database home is not available on the passive node until failover occurs.

S-TAP can be configured for delayed loading by setting a configuration file property, `WAIT_FOR_DB_EXEC`. When S-TAP restarts, either from a system reboot or user initiated S-TAP stop / start commands, S-TAP polls all databases that have been configured to be monitored and begins monitoring all valid configurations. Any configuration anomalies (either on the database side or the S-TAP side) that limits S-TAP ability to monitor a database does not limit the S-TAP from monitoring other databases with valid configurations. This parameter determines the S-TAP response, and its status in the S-TAP Control page, if a DB instance is not available (`db_install_dir` or `db_exec_file` is not accessible) during IE validation, after an S-TAP or DB restart.

- 0 and less: S-TAP logs an event message with the event type `CONF_ERROR` when a DB instance is detected as unavailable for certain DB(PROTOCOL) during the S-TAP starting time. S-TAP also logs a `CONF_ERROR` if a DB changes its status from available to unavailable during the periodic check (every 15 minutes). These event messages change the S-TAP status in the GUI to yellow with the instruction to correct the parameter or set `WAIT_FOR_DB_EXEC > 0`. When a DB instance status changes from unavailable to available, a `WARNING` message is sent to the sniffer, but the GUI status does not change automatically. You need to click  to open the S-TAP event log and click Accept.
- greater than 0: A `WARNING` is logged for any unavailable database during S-TAP startup time or during a periodic check. The time interval of the periodic check is the value of `wait_for_db_exec`, in minutes. A warning message is also sent when an unavailable DB instance becomes available. Since the periodic check needs to get status of the database file configured for each inspection engine, and it consumes the CPUs, the value should not be less than the number of inspection engines.

Before setting this property to a positive value, be sure to set all other necessary configuration properties and test that the S-TAP starts and collects data correctly. This property can be modified using GIM GUI (`STAP_WAIT_FOR_DB_EXEC`), and the `guard_tap.ini` configuration file. It cannot be modified in the S-TAP Control UI page.

## Linux-UNIX: What to restart or reboot on the database server after installing or updating S-TAP

This topic details what needs to be rebooted or restarted after you install or upgrade your UNIX or Linux S-TAP. Restart and reboot requirements are the same for GIM and non-GIM implementations.

### Installing S-TAP when using EXIT

Db2 and Teradata: No restart needed.

Informix: No restart needed. If ifxserver is running, then restart it. If ifxserver is not running, then you do not need to restart anything.

### Installing S-TAP when using A-TAP

The database must be restarted when using A-TAP.

Deactivate and de-instrument the A-TAP before any database software updates.

### Installing S-TAP when using K-TAP with TCP/IPC or shared memory connections (SHM)

| OS/Database | Oracle  |     | Db2     |     | Sybase  |     | Mysql   |     | Informix |     |
|-------------|---------|-----|---------|-----|---------|-----|---------|-----|----------|-----|
|             | TPC/IPC | SHM | TPC/IPC | SHM | TPC/IPC | SHM | TPC/IPC | SHM | TPC/IPC  | SHM |
| Linux       | NR      | NR  | NR      | REQ | NR      | NR  | NR      | NA  | NR       | REQ |
| AIX *       | REQ     | NR  | REQ     | NR  | REQ     | NR  | REQ     | NA  | REQ      | NR  |
| Solaris     | NR      | NR  | NR      | NR  | NR      | NR  | NR      | NA  | NR       | NR  |
| HP-UX       | NR      | NR  | NR      | NR  | NR      | NR  | NR      | NA  | NR       | NR  |

Where:

- NR = No restart/reboot required (based on utilizing live update mechanism and referencing live update link if you have one)
- REQ = Restart required
- NA = Not applicable

\* On AIX, a database restart is always required after you install S-TAP in order to capture TCP traffic. When you install an S-TAP on AIX, AIX updates the system calls. When you restart the database server, K-TAP intercepts and updates the system call to ensure the server can access the most current system call.

### What to restart after a live upgrade of UNIX/Linux S-TAP

No restarts are necessary at all for live upgrades that do not include A-TAP or exit libraries.

Deactivate and de-instrument the A-TAP prior to any S-TAP upgrades.

#### When using Exit libraries:

- If you upgrade from v10.6.0.0 and higher, you do not need to restart the database. You can upgrade the S-TAP while the database is running; the next time the database is restarted, the updated exit library is used.
- If you upgrade from any release before 10.6.0.0: Restart any databases that use an exit library.

### Reboot guidelines

Rebooting the database server is only required when uninstalling K-TAP (whether or not K-TAP is in use).

## Linux-UNIX: Managing a GIM-, RPM-, and shell-installed S-TAP during a database upgrade

Only the A-TAP needs handling when you upgrade a database with a GIM, RPM, or shell-installed UNIX S-TAP. If a system is running multiple databases, the S-TAP can continue to run and monitor all other databases not being upgraded.

## Procedure

1. De-instrument, and de-activate the A-TAP, by using the guardctl utility.
2. Upgrade your database.
3. Instrument, activate, and restart the A-TAP, by using the guardctl utility.
4. If the system uses exit libraries, make sure that the exit library is in the appropriate place (for example if the DB location directory changed).
5. Verify that the inspection engine is correct, because paths may have changed.

When the DBA upgrades the database with a different installation path than the previous version, traffic is not captured unless you update with the correct installation path and restart the S-TAP. If the installation path is not updated, the database might not be monitored. Look in the S-TAP Events report for a message:  
DB instance stops running, please make sure DB under db\_install\_dir is still available, and restart the relevant S-TAP. If found, update db\_install\_dir in the guard\_tap.ini or DB Install Dir in the S-TAP control page.

6. Check that the inspection engine for the database is correct (for example, the version number).
7. If you modified the inspection engine configuration, including the DB installation path, restart the S-TAP.

## Related concepts

- [Linux-UNIX: guardctl return codes](#)

## Related reference

- [Linux-UNIX: guardctl utility commands for A-TAP](#)
- [Linux-UNIX: Database-specific guardctl parameters](#)

# Linux-UNIX: Managing GIM clients during a major upgrade of the database server operating system

When you upgrade the operating system on your database server, use the GIM client to automatically upgrade itself and the GIM bundles (for example, GIM, S-TAP, CAS) installed on the Linux-UNIX database. However, most operating systems do not support a major upgrade, for example from RHEL7 to RHEL8.

## Before you begin

The target upgrade GIM bundles must be available on the GIM server. The build number of each bundle must be the same or greater than the bundle that is installed. Download from [Fix Central](#).

## About this task

This procedure is only relevant for databases whose operating system can be upgraded. If you cannot upgrade the operating system, you must uninstall the S-TAP, install the new operating system, and install the S-TAP bundle that is compatible with the newly installed operating system.

GIM bundles are OSType/OsVersion/Processor specific. When the OS version changes (for example, from RHEL7 to RHEL8), all the bundles need to be upgraded.

The GIM parameter auto\_install\_on\_db\_server\_os\_upgrade controls GIM's ability to auto-upgrade all bundles. If enabled, when the database server boots up after an operating system upgrade, GIM automatically downloads and installs these bundles. This parameter is disabled by default, to prevent unintentional bundle upgrades.

If the parameter is disabled when you upgrade the database operating system, the GIM client detects that the operating system changed, and it changes the \_x suffix of the version to \_0. You can see the version in the Set up by Client, for example, 10.6.1.4\_r123456\_0. To resolve the mismatch between the GIM client and the database operating system, do one of:

- Enable the GIM global parameter auto\_install\_on\_db\_server\_os\_upgrade, which automatically upgrades all the GIM clients with the latest bundle of the operating system they support.
- Do not enable auto\_install\_on\_db\_server\_os\_upgrade, and upgrade the GIM clients manually.

It is best to update all your GIM-installed modules as soon as possible after the upgrade, whether manually or automatically. K-TAP is not loaded after an operating system upgrade.

## Procedure

1. Log in to the CLI of the Guardium system that is the GIM server
2. Enable auto\_install\_on\_db\_server\_os\_upgrade by entering:

```
grdapic gim_set_global_param paramName="auto_install_on_db_server_os_upgrade" paramValue="1"
```

3. Upgrade the operating system on your database server.

## Results

At first boot after OS upgrade, the GIM client recognizes that the operating system was upgraded and:

1. Changes the configuration files for all GIM-installed modules to support the new operating system attributes.
2. Registers all the modules to the GIM server with the updated attributes. This change triggers the GIM server to look for a bundle that has the same build number as the previously installed bundle, but is compatible with the upgraded operating system. If it does not find such a bundle, it looks for the latest bundles that support the new operating system attributes. When the server finds appropriate bundles, it schedules them for upgrade and runs the upgrade process immediately. If the server cannot find appropriate bundles, it issues an error message.
3. Records an alert in the GIM\_EVENTS report, that an operating system upgrade occurred and lists the actions that should be taken.

## What to do next

Review the messages in the GIM\_EVENTS report. If the GIM server reports that the modules were upgraded successfully, verify the proper operation of the modules as you would do after any update.

If error messages were written to the GIM\_EVENTS report, indicating that the upgrade was not successful, review the error messages for guidance.

When the operating system upgrade is complete, disable the automatic update option on the GIM server to prevent a GIM client from erroneously starting an update process.

```
grdapic gim_set_global_param paramName="auto_install_on_db_server_os_upgrade" paramValue="0"
```

# Linux-UNIX: Managing an RPM- or shell-installed S-TAP during a major upgrade of the database server operating system

When you upgrade the operating system on your database server, you need to uninstall the S-TAP, and install a new version. However, most operating systems do not support a major upgrade, for example, from RHEL7 to RHEL8.

## Before you begin

The appropriate target upgrade shell or RPM bundles must be available on the database. The build number of each bundle must be the same or greater than the bundle that is installed. Download from [Fix Central](#).

## About this task

---

If you cannot upgrade the operating system, you must uninstall the S-TAP, install the new operating system, and install the S-TAP bundle that is compatible with the newly installed operating system.

## Procedure

---

1. Log in to the database.
2. If the system uses A-TAP: Disable and deinstrument the A-TAP by using the `guardctl` utility.
3. Uninstall the S-TAP, which also uninstalls the K-TAP.
4. Upgrade the operating system on your database server. (Upgrading includes at least one reboot of the operating system.)  
Note: Before you reboot, make sure to set the `ktap_installed` parameter to 1.
5. Install the S-TAP and the K-TAP with the appropriate installer.  
For example, if you are upgrading from RHEL7 to RHEL8, you used the RHEL7 to uninstall the S-TAP in step 3, but you need the RHEL8 installer to install the new S-TAP.
6. If the system uses A-TAP: Instrument and enable the A-TAP by using the `guardctl` utility.

## Related concepts

---

- [Linux-UNIX: Preparing to install K-TAP](#)
- [Linux-UNIX: S-TAP compilation of K-TAP](#)
- [Linux-UNIX: guardctl return codes](#)

## Related tasks

---

- [Linux-UNIX: Requesting a K-TAP module](#)

## Related reference

---

- [Linux-UNIX: guardctl utility commands for A-TAP](#)
- [Linux-UNIX: Database-specific guardctl parameters](#)

# Linux-UNIX: Managing a GIM-, RPM-, or shell-installed S-TAP during a minor or kernel upgrade of the database server operating system

A minor database operating system upgrade can include a new operating system kernel. Use this task for both a minor upgrade or a kernel upgrade.

## Before you begin

---

- The loader automatically picks the right K-TAP at boot time.
- If the new kernel is already supported by a K-TAP module, the K-TAP installs as part of the S-TAP installation.
- If the new kernel is not supported by a K-TAP module, then you must install the development packages that support a local K-TAP module build. You might need to request a new K-TAP module from IBM Support. Save the appropriate K-TAP module locally on the database. For more information, see [Linux-UNIX: Preparing to install K-TAP](#).
- The parameter `auto_install_on_db_server_os_upgrade` is not relevant in this scenario.

## Procedure

---

1. If the system uses A-TAP: Use the `guardctl` utility to disable and deinstrument the A-TAP.
2. Upgrade the operating system or the kernel on your database server (upgrading includes rebooting the operating system.).  
Note: Before you reboot, make sure that the `ktap_installed` parameter in `guard_tap.ini` is set to 1.
3. If the system uses A-TAP: Use `guardctl` to instrument and enable the A-TAP.

## Related concepts

---

- [Linux-UNIX: Preparing to install K-TAP](#)
- [Linux-UNIX: S-TAP compilation of K-TAP](#)
- [Linux-UNIX: guardctl return codes](#)

## Related tasks

---

- [Linux-UNIX: Requesting a K-TAP module](#)

## Related reference

---

- [Linux-UNIX: guardctl utility commands for A-TAP](#)

- [Linux-UNIX: Database-specific guardctl parameters](#)

## Linux-UNIX: Configuring S-TAP

Learn to configure the S-TAP.

To configure an S-TAP, you need to make changes to the guard\_tap.ini file that resides in the S-TAP default directory under /usr/local/guardium.

When you make changes to an S-TAP, Guardium updates the following files:

- guard\_tap.ini - The current working S-TAP configuration file.
- guard\_tap.ini.default\_orig - The default guard\_tap.ini file
- guard\_tap.ini.save\_default - The default file saved before you make any configuration changes.
- guard\_tap.ini.err - S-TAP configuration error log file.
- guard\_tap.ini.bak - This file is updated with the last successfully saved S-TAP configuration that passes parameters validation.
- guard\_tap.ini.prev - This file is updated with the last successfully saved S-TAP configuration that passes parameters validation and starts the S-TAP without error.

In general, you never need to touch the guard\_tap.ini files. You can configure the S-TAP either in the GUI or by using the **guard\_config\_update** command.

- [Linux-UNIX: Configuring S-TAP in the S-TAP Control page](#)

In the S-TAP Control page you can view all S-TAPs managed by this Guardium system, manage individual S-TAPs, and perform a few operations on all S-TAPs.

- [Linux-UNIX: Scheduling S-TAP diagnostics](#)

12.1 and later You can schedule S-TAP diagnostics by using the S-TAP Diagnostic Scheduler user interface.

- [Linux-UNIX: Configure S-TAP with guard-config-update](#)

You can use the guard-config-update script to update your S-TAP configuration (without using the GUI), whether S-TAP was installed with GIM, RPM, or shell.

- [Linux-UNIX: Discover database instances](#)

Enable S-TAP to periodically discover database instances and send the results to the current active S-TAP system.

- [Linux-UNIX: Configuring an Inspection Engine](#)

Configure or modify an inspection engine in the S-TAP Control pane.

- [Linux-UNIX: Inspection engine verification](#)

S-TAP verification confirms that the S-TAPs and their inspection engines in your environment are running and actively monitoring database activity. Understand verification, and define a schedule to regularly verify S-TAPs.

- [Linux-UNIX: S-TAP load-balancing models and configuration guidelines](#)

Understand the S-TAP load-balancing models, and choose the one appropriate to your setup.

- [Linux-UNIX: Kerberos-authenticated database traffic](#)

Kerberos is a network authentication protocol that eliminates the transmission of unencrypted passwords across the network.

- [Linux-UNIX: A-TAP management](#)

A-TAP is an application-level tap. It sits in the application layer to support monitoring of encrypted database traffic, which cannot be done in the kernel by K-TAP.

- [Linux-UNIX: Configure a public and private address for an S-TAP](#)

For an S-TAP deployed in a private network, Guardium® can refer to the S-TAP with a public IP address that is not visible from the database server on which S-TAP is installed, while the database uses a private address for the S-TAP.

- [Linux-UNIX: Configure S-TAP log and dump locations when /root partition size is limited](#)

S-TAP agents are installed in a partition with root privileges; by default they are installed into the /root partition based directories. For customers with limited root file systems size, follow these best practice recommendations to prevent the S-TAP agent from generating logs or dumps on the /root partition.

- [Linux-UNIX: Editing the S-TAP configuration parameters](#)

You can modify the S-TAP configuration after it is installed using GIM, the UI, or for advanced users, the configuration file on the database.

## Linux-UNIX: Configuring S-TAP in the S-TAP Control page

In the S-TAP Control page you can view all S-TAPs managed by this Guardium system, manage individual S-TAPs, and perform a few operations on all S-TAPs.

### Before you begin

You must be logged in to the Guardium system that is the active host for the S-TAP.

### About this task

Sometimes a user is unable to decide during the process of installing an S-TAP or can make the wrong decision and it goes undetected until after the installation process is complete. For instance, a user can forget to type in or use the wrong IP address for the SQL Guard IP. These types of mistakes can be remedied by modifying the S-TAP configurations.

Parameters in the GUI can be safely changed. Parameters that are not in the GUI rarely need changing and should normally be left unmodified; they are for use by Guardium Technical Support or advanced users.

All configuration changes require that the S-TAP agent be restarted. If you modify parameters in the GUI or with GIM, the S-TAP is restarted transparently. If you need to restart the S-TAP manually (for example after modifying the configuration by API or directly in the guard\_tap.ini), use the [Send Command](#) or follow the direction in [Linux-UNIX: Start and stop S-TAP and GIM processes for various OS types/versions](#) or [Linux-UNIX: Using guard-config-update to start, restart, and stop S-TAP, and view status](#).

If you installed your S-TAP by using the Guardium Installation Manager (GIM), you can update some parameters through the GIM GUI.

S-TAP status can be one of:

- Green: Online
- Yellow: one of:
  - Configuration error: When you modify S-TAP parameters in the GUI or GuardAPI, S-TAP checks the values before saving the parameters. When the S-TAP identifies an erroneous value, it does not save it and it creates an error in the S-TAP event log. The S-TAP uses default values so that it can keep sending

traffic. The S-TAP creates a backup guard\_tap.ini.bak under the S-TAP directory when it corrects the configuration. Click  to open the S-TAP event log, and evaluate the LOG\_CONF\_ERR error. Click one of the options:

- Accept to save the value the S-TAP assigned to the parameter
- Modify to open the Modify Configuration dialog and change the value.
- Close to close the window without making any changes or accepting the value.

(Parameters that do not have defaults, such as DB Install Dir and Process Name, do not have the accept option.) After you either accept or modify to a valid value, the status becomes green and the timestamp is updated. The S-TAP creates a backup guard\_tap.ini when it corrects the configuration. It is saved as guard\_tap.ini.bak under the S-TAP directory.

- Warning: After an S-TAP restart either db\_install\_dir or db\_exec\_file is not accessible during inspection engine validation. Guardium periodically checks for S-TAP status.

- Red: Offline

## Procedure

1. Go to Manage > Activity Monitoring > S-TAP Control to open S-TAP Control.
2. Perform operations on all S-TAPs in the page.
  - Refresh: refresh display of S-TAPs.
  - Add All to Schedule: add all displayed S-TAPs to the S-TAP verification schedule. See [Linux-UNIX: Inspection engine verification](#).
  - Remove All from Schedule: remove all displayed S-TAPs from the S-TAP verification schedule.
  - Comments: add comments. See [Comments](#).
3. Identify the S-TAP to be configured by its IP address or the symbolic hostname of the database server on which it is installed. View and perform operations on individual S-TAPs.

| Option                                                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>Click Delete to remove an S-TAP.</p> <p>Delete an S-TAPs if you know that an S-TAP is inactive, or when the Guardium unit is no longer listed as a host in the S-TAPs configuration file. In either of these cases, the S-TAP displays indefinitely with an offline status if you do not delete it. (See also <a href="#">Linux-UNIX: Deleting inactive S-TAPs in a centralized environment</a>.)</p> <p>You cannot delete an active S-TAP from the list.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|    | Click Refresh to fetch a copy of the latest S-TAP configuration from the agent. (The S-TAP display does not auto-refresh.)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|  | <p>Opens the S-TAP Commands pop-up, where you can run various commands on the S-TAP host.</p> <ul style="list-style-type: none"> <li>• Restart. Action depends on the Restart Mode.</li> <li>• Restart. Retsarts the S-TAP in the mode you select.           <ul style="list-style-type: none"> <li>• 0: Restarts the S-TAP. Use this mode in environments without enterprise load balancing.</li> <li>• 1: Restarts the S-TAP process while preserving the data in the S-TAP buffer. (The S-TAP picks up the new configuration from the enterprise load balancer without flushing the buffers.) Used in the enterprise load balancer environment.</li> </ul> </li> <li>• S-TAP logging: Starts S-TAP logging for debugging purposes, at the log level you enter in Level and for the duration you enter in Duration Sec. See tap_debug_output_level in <a href="#">Linux-UNIX: Debug parameters</a>.</li> <li>• Reinitialize buffer: Reset the K-TAP statistics along with deleting the S-TAP buffer.</li> <li>• K-TAP logging: Similar to S-TAP Logging; increases the debug output from K-TAP.</li> <li>• Push Guardium Insights Trust: To use an S-TAP to stream data from Guardium® Data Protection to Guardium Insights, you must first make establish trust. Use Push Guardium Insights Trust to paste in a signed, trusted Guardium Insights certificate . The certificate must be in PEM format and include the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- tags. From the CLI, you can use the <a href="#">push_insights_trust</a> API to push the certificate.</li> <li>• Run Diagnostics: Run the S-TAP diagnostics script (and upload the results to the Guardium system)</li> <li>• Upload Linux Modules: Linux only. Uploads the local custom build module of K-TAP.</li> <li>• Store SQL credentials: Saves the username - password pair on the selected S-TAP. (The password is encrypted on the S-TAP.) The S-TAP uses these credentials to access a database. See <a href="#">Linux-UNIX: Configuring S-TAP interception using Oracle Unified Audit</a>.</li> <li>• Revoke Ignore: All sessions that are ignored by a revocable ignore policy become unignored, and S-TAP starts capturing the traffic for those sessions.</li> <li>• Run Database Instance Discovery: Runs the discovery process once, immediately. (If enabled to run automatically, it runs, by default, every 24 hours.) You can specify rules to manage database instance discovery. To use discovered instance rules, clear the Replace Inspection Engines checkbox. For more information, see <a href="#">Database discovered instances rules</a>.</li> </ul> |
|  | <p>Opens the S-TAP configuration window. Parameters that do not appear in the GUI are advanced parameters. Do not modify them unless you are an advanced user, or Guardium Technical Support instructs you to modify them. See GUI parameters:</p> <ul style="list-style-type: none"> <li>• <a href="#">Linux-UNIX: S-TAP Control: Details</a></li> <li>• <a href="#">Linux-UNIX: S-TAP Control: Change auditing parameters</a></li> <li>• <a href="#">Linux-UNIX: S-TAP Control: Application server user identification parameters</a></li> <li>• <a href="#">Linux-UNIX: S-TAP Control: Guardium Hosts parameters</a></li> <li>• <a href="#">Linux-UNIX: S-TAP Control: Firewall parameters</a></li> <li>• <a href="#">Linux-UNIX: S-TAP Control: Inspection engine parameters</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|  | <p>Click to open the S-TAP event log, where you can see events such as connect, disconnect, GIM server configuration. This log is useful for troubleshooting. As described in <a href="#">S-TAP status</a>, use the event log to identify configuration errors (LOG_CONF_ERR).</p> <p>You can:</p> <ul style="list-style-type: none"> <li>• Accept to save the value the S-TAP assigned to the parameter</li> <li>• Modify to open the Modify Configuration dialog and change the value.</li> <li>• Close to close the window without making any changes or accepting the value.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|  | Adds the individual S-TAP to the scheduled verification.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|  | A database might be running many sessions, some of which are currently ignored. Clear this option to stop ignoring traffic from ignored sessions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

- [\*\*Linux-UNIX: S-TAP Control: Details\*\*](#)

These parameters define basic properties of the S-TAP. This topic lists the full set of parameters that can display under Details. Not all parameters display for every type of database server.

- [\*\*Linux-UNIX: S-TAP Control: Change auditing parameters\*\*](#)

These parameters affect the behavior of CAS.

- [\*\*Linux-UNIX: S-TAP Control: Application server user identification parameters\*\*](#)

These parameters affect the behavior of the S-TAP when an application user name needs to be bounded with database activities.

- [\*\*Linux-UNIX: S-TAP Control: Guardium Hosts parameters\*\*](#)

These parameters describe a Guardium system to which this S-TAP can connect.

- [\*\*Linux-UNIX: S-TAP Control: Firewall parameters\*\*](#)

These parameters affect the behavior of the S-TAP with respect to the firewall.

- [\*\*Linux-UNIX: S-TAP Control: Inspection engine parameters\*\*](#)

These parameters affect the behavior of the inspection engine that the S-TAP uses to monitor a data repository on a DB server. You can define up to 50 inspection engines per S-TAP.

---

## Linux-UNIX: S-TAP Control: Details

These parameters define basic properties of the S-TAP. This topic lists the full set of parameters that can display under Details. Not all parameters display for every type of database server.

Table 1. S-TAP Control: Details parameters

| Name                            | Default value | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version                         |               | Read only. The S-TAP version that is installed on the DB server, added to the file during installation or upgrade only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Devices                         | none          | Which interfaces to listen on. Use <b>ifconfig</b> to find the correct interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Load balancing                  | 0             | <p>Controls load balancing to Guardium® systems. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: No load balancing.</li> <li>• 1: Load balancing. Traffic is balanced between the primary and secondary servers, which are defined in the SQLGuard section.</li> <li>• 2: Redundancy. Fully mirrored S-TAP sends all traffic to all primary and secondary servers, which are defined in the SQLGuard section.</li> <li>• 3: Hardware load balancing. Guardium uses a load balancer such as F5 or Cisco. S-TAP sends the traffic to the load balancer, which forwards it to one of the collectors in the pool.</li> <li>• 4: Multiple KTAP buffer and S-TAP threads are used to split the traffic.</li> </ul> <p>Use the primary parameter in the SQLGUARD section to specify primary, secondary, tertiary or more, servers. If this parameter is set to 0, and you have more than one Guardium system monitoring traffic, then the non-primary Guardium systems are available for failover.</p> <p>This parameter is also used in enterprise load balancing. For more information, see <a href="#">Enabling enterprise load balancing and associating an S-TAP with a central manager</a>.</p> |
| Messages remote                 |               | <p>Send messages to the active Guardium host.</p> <ul style="list-style-type: none"> <li>• <input checked="" type="checkbox"/> : enabled.</li> <li>• <input type="checkbox"/> : disabled.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Messages syslog                 |               | <p>Send messages to syslog.</p> <ul style="list-style-type: none"> <li>• <input type="checkbox"/> : Disabled.</li> <li>• <input checked="" type="checkbox"/> : Enabled.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Trace files dir                 |               | The directory in which access tracer files are stored.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Alternate ips                   | NULL          | Comma-separated list of alternate or virtual IP addresses used to connect to this database server. The alternate_ips parameter is only used when your server has multiple network cards with multiple IPs, or virtual IPs. S-TAP only monitors traffic when the destination IP matches either the S-TAP Host IP defined for this S-TAP, or one of the specified alternate IPs. It's recommended that you specify all virtual IPs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| App. Server User Identification |               | <p>Valid values:</p> <ul style="list-style-type: none"> <li>• 0 S-TAP acts as normal</li> <li>• 1: S-TAP is set in 'client mode', switches S2C and C2S packets to reflect S-TAP being installed on client, not the DB server. Checks if the other appserver_* parameters are specified. If they are defined, examines HTTP packets on the supplied port to take session information about the end user of the java-application that is installed on the client system.</li> </ul> <p>Default: 0</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| TLS                             |               | <p>Select the checkbox to use SSL to encrypt traffic between the S-TAP and the Guardium system. This adds ~15% of CPU usage to the sniffer's S-TAP server but does not affect the sniffer's other modules.</p> <p>Guardium recommends encrypting network traffic between the S-TAP and the collector whenever possible: only in cases where the performance is a higher priority than security should this be disabled. If unencrypted, the traffic between the S-TAP agent and Guardium system is in clear text.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Compres. Level                  | 0             | <p>Increase the compression level to lower the number of bytes between the S-TAP and the collector. Changing the compression level is recommended where latency is high between the data centers, to reduce travel time. Compression might impact performance on both ends (S-TAP and collector (sniffer)). The disk usage is not affected by compression. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: No compression</li> <li>• 1: Best speed</li> <li>• 9: Highest compression</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

| Name                                          | Default value                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All can control                               | <input checked="" type="checkbox"/> | Defines which Guardium system control this S-TAP. Valid values: <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> S-TAP is controlled by the primary Guardium system only.</li> <li><input checked="" type="checkbox"/> S-TAP can be controlled by any Guardium system.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Load balancer host name or IP address         |                                     | Required for enterprise load balancing. If blank, enterprise load balancing is disabled. The IP address or hostname of the central manager or managed unit this S-TAP uses for load balancing.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Managed Units                                 | 1                                   | The number of managed units the enterprise load balancer allocates for this S-TAP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Include client IP in UID chain for SSH daemon | <input checked="" type="checkbox"/> | Add an SSH client IP:port pair to the UID chain when SSH is identified as one of the processes in the chain. Valid values: <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Disabled.</li> <li><input checked="" type="checkbox"/> Enabled.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| OS type                                       |                                     | Read only. Software version running on the database.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| DB request handler                            | <input checked="" type="checkbox"/> | Allow the database to access K-TAP without manual configuration (requires a defined DB user in the Inspection Engines section). <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Disabled.</li> <li><input checked="" type="checkbox"/> Enabled.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Cassandra audit                               | <input checked="" type="checkbox"/> | Create a file appender pipe for Cassandra/Datastax with native audit logging. Valid values: <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Disabled.</li> <li><input checked="" type="checkbox"/> Enabled.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Cassandra audit delimiter                     | GUARD_DELIM                         | Cassandra audit reader delimiter. Valid values: <ul style="list-style-type: none"> <li>printable ASCII characters a-z A-Z 0-9 - _ ! @ # \$ % ^ &amp; * ()</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Restricted logging                            | 0                                   | Controls restricted logging on the collector. Use this to evaluate the number of records affected by an SQL command, while masking the actual query. This parameter can only be set by user root on the DB server. Valid values: <ul style="list-style-type: none"> <li>0: Unrestricted.</li> <li>1: Log with masking. Only logins are allowed (sent packets are flagged with LOGALWAYSMASK). Forces encryption to be on in the S-TAP regardless of any other settings; traffic is sent to the collector only after the collector has indicated that it is aware of the parameter value. Otherwise, the S-TAP logs a message that traffic can't be sent, and its status is red in the S-TAP Control page.</li> <li>2: All packets are allowed (sent packets are flagged with LOGACCESSIONLY)</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| SQL configuration properties directory        |                                     | Relevant for Oracle Unified Auditing. The path to the tnsnames.ora file that describes the connections to the database to be monitored.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| LD library paths                              |                                     | Relevant for Oracle Unified Auditing. The path to the Oracle Instant Client libraries installed on the system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Discovery interval                            |                                     | The interval at which the S-TAP reports database instance discovery results to the collector. Select only if you want to change the discovery interval from its default of 24 hours. When you select this option, the UI updates with two radio buttons: Hour and Minute. Type in any positive integer to set the discovery interval in either hours or minutes. Clear the Enable discovery interval checkbox to disable.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Wait for DB exec                              |                                     | When S-TAP restarts, either from a system reboot or user initiated S-TAP stop / start commands, S-TAP polls all databases that have been configured to be monitored and begins monitoring all valid configurations. Any configuration anomalies (either on the database side or the S-TAP side) that limits S-TAP ability to monitor a database does not limit the S-TAP from monitoring other databases with valid configurations. This parameter determines the S-TAP response, and its status in the S-TAP Control page, if a DB instance is not available (db_install_dir or db_exec_file is not accessible) during IE validation, after an S-TAP or DB restart. <ul style="list-style-type: none"> <li>0 and less: S-TAP logs an event message with the event type CONF_ERROR when a DB instance is detected as unavailable for certain DB(PROTOCOL) during the S-TAP starting time. S-TAP also logs a CONF_ERROR if a DB changes its status from available to unavailable during the periodic check (every 15 minutes). These event messages change the S-TAP status in the GUI to yellow with the instruction to correct the parameter or set WAIT_FOR_DB_EXEC &gt; 0. When a DB instance status changes from unavailable to available, a WARNING message is sent to the sniffer, but the GUI status does not change automatically. You need to click  to open the S-TAP event log and click Accept.</li> <li>greater than 0: A WARNING is logged for any unavailable database during S-TAP startup time or during a periodic check. The time interval of the periodic check is the value of wait_for_db_exec, in minutes. A warning message is also sent when an unavailable DB instance becomes available. Since the periodic check needs to get status of the database file configured for each inspection engine, and it consumes the CPUs, the value should not be less than the number of inspection engines.</li> </ul> |
| Kerberos plugin directory                     |                                     | Location of the Kerberos file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Force server IP                               |                                     | Forces the reported server IP of database to be the S-TAP Host value. Valid values: <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Disabled.</li> <li><input checked="" type="checkbox"/> Enabled.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Private tap IP                                |                                     | If this parameter is defined, the database uses it for the S-TAP communication. (Relevant when the S-TAP is deployed in a private network; the external, public IP address of the S-TAP is defined by tap_ip. See <a href="#">Linux-UNIX: Configure a public and private address for an S-TAP</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Name                                      | Default value | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dynamic ring buffers                      | ✗             | Dynamically adds and removes S-TAP buffers for each main connection during peak traffic, to prevent an overflow in the S-TAP buffer. If S-TAP failover happens, data in all buffers is moved to the new buffers.<br>Valid values: <ul style="list-style-type: none"><li>• ✗: Disabled.</li><li>• ✓: Enabled.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 12.1 and later K-TAP Dynamic ring buffers | ✗             | Dynamically adds and removes K-TAP buffers for each main connection during peak traffic period, to prevent an overflow in the K-TAP buffer.<br>Valid values: <ul style="list-style-type: none"><li>• ✗: Disabled.</li><li>• ✓: Enabled.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| KTAP fast TCP verdict                     | 1             | For TCP connections. Valid values: <ul style="list-style-type: none"><li>• 0: slow verdict. K-TAP sends information about the session to STAP to ask whether or not the traffic should be intercepted.</li><li>• 1: fast verdict. K-TAP decides on its own.</li></ul> In both cases, the network/exclude network parameters are checked against the incoming IP. From 10.1.4, the value is 1 after upgrade.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| KTAP fast file verdict                    | 1             | Push file information to K-TAP for determining if pipe traffic should be intercepted. For TLI connection, K-TAP sends ioctl to the S-TAP to confirm that the session is the database connection configured in the IE by checking ports and IPs, when ktap_fast_file_verdict is set to 1, then K-TAP does not send the request to the S-TAP as long as the session's ports are in the range.<br>Valid values: <ul style="list-style-type: none"><li>• 0: No</li><li>• 1: Yes</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| KTAP fast shmem                           | ✓             | Push shmem information to K-TAP to determine if shmem traffic should be intercepted. Valid values <ul style="list-style-type: none"><li>• ✗: Disabled.</li><li>• ✓: Enabled.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| KTAP local TCP                            | ✗             | This parameter is used for TCP connections. <ul style="list-style-type: none"><li>• ✗: Intercept all connections.</li><li>• ✓: Only intercept local connections (although previously intercepted connections are still captured)</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| QRW installed                             | 0             | Enable or disable the query rewrite feature. When set to 0, all other parameters in this group are ignored. Valid values: <ul style="list-style-type: none"><li>• 0: Disabled</li><li>• 1: Enabled</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| QRW default state                         | 0             | Sets the query rewrite activation trigger. Must be 0 if firewall_default_state=1. Valid values: <ul style="list-style-type: none"><li>• 0: QRW activated per session when triggered by a rule in the installed policy</li><li>• 1: QRW activated for every session regardless of the installed policy.</li><li>• 2: All traffic is watched by default for QRW policy violations, but if no event triggers the watch in the first PRIORITY_COUNT packets, query rewrite is turned off for the session.</li></ul> When set to 2, the QRW operation can be modified by the following commands: <b>Watch</b> , <b>Drop</b> , <b>Watch &amp; Drop</b> and <b>Unwatch</b> . When a <b>Watch</b> command is received while state 2 is in effect, it changes the state from 2 to 1 so that the connection is permanently subject to firewall or query rewrite operations. When a <b>Drop</b> or <b>Watch &amp; Drop</b> is received, the connection is immediately terminated. When an <b>Unwatch</b> command is received while state 2 is in effect, it changes the state from 2 to 0 so the connection is no longer subject to firewall or query rewrite operations. |
| QRW force watch                           | NULL          | Comma-separated list of client IP/MASKs (for example, 1.1.1.1/1.1.1.1.2.2.2.2/2.2.2.2) to watch automatically. Valid when qrw_installed is 1, and qrw_default_state is 0. Cannot be configured to the same IP range as firewall_force_unwatch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| QRW force unwatch                         | NULL          | Comma separated list of client IP/MASKs (for example, 1.1.1.1/1.1.1.1.2.2.2.2/2.2.2.2) to exclude from watching. Valid when qrw_installed is 1, and qrw_default_state is 1. Cannot be configured to the same IP range as firewall_force_unwatch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Hunter trace                              | ✗             | Turns on the collection of UID chains. When enabled, captures the UID but without IP in the string. Use this setting for local TCP/IP connections including Solaris zones and AIX WPARs, and remote TCP/IP connections when appserver_installed = 1. <ul style="list-style-type: none"><li>• ✗: Disabled.</li><li>• ✓: Enabled.</li></ul> See more information in <a href="#">Linux-UNIX: UID chains</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Load balancer node affinity               | ✗             | Whether the S-TAP connects to more than one managed unit, for enterprise load balancing. Some scenarios need all traffic to go to the same collector. With Oracle ATAP, for example, the analyzed client IP only shows if both the encrypted and unencrypted sessions go to the same managed unit. <ul style="list-style-type: none"><li>• ✗: Disabled. The S-TAP traffic goes to, at a maximum, the number of managed units specified by Managed Units.</li><li>• ✓: Enabled. The S-TAP traffic goes to one managed unit, and has, at a maximum, the number of connections (to that managed unit) specified by Managed Units.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

| Name                      | Default value | Description                                                                                                                                                                                                                                                                                                                                      |
|---------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Discovery use port ranges | ✗             | Enable S-TAP discovery of Oracle databases to combine discovered instances based on port ranges. This setting works with a single unix_domain_socket_marker. Multiple unix_domain_socket_marker configurations require separate instances.<br>Valid values: <ul style="list-style-type: none"><li>• ✗: Disabled.</li><li>• ✓: Enabled.</li></ul> |

## Related concepts

- [Linux-UNIX: S-TAP load-balancing models and configuration guidelines](#)
- [Linux-UNIX: Discover database instances](#)
- [Linux-UNIX: UID chains](#)

## Linux-UNIX: S-TAP Control: Change auditing parameters

These parameters affect the behavior of CAS.

Table 1. CAS parameters for UNIX/Linux

| Name                      | Default value     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Task checkpoint           | task_checkpoint   | Internal handle program machine state in case of host failure.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Client checkpoint         | client_checkpoint | File used to restart processing. A series of files is created. Each version of the file ends with a unique number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Checkpoint period         | 60                | Interval time, in seconds, for the check.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Fail over file            | fail_over_file    | Name of the outgoing messages buffer. The database writes to this file when the Guardium® system cannot be reached. During this time, the file can grow to the maximum size specified. When the limit is reached, a second file is created, with the same name with the digit 2 appended to the end of the name. (At this point CAS begins trying to connect to a secondary server.) If that file also reaches the maximum size, the first file is overwritten. If the first file fills again, the second file is overwritten. Thus, following an extended outage, you might lose data, but an amount of data up to twice the size of the Failover File Size Limit is stored. |
| Fail over file size limit | 50000             | Failover file maximum size, in KB. The disk space requirement is twice what you specify here because the system maintains two failover files. If you specify -1, the file size is unlimited, but it is recommended that you cap the file size.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Max rec. attempts         | 5000              | Number of reconnect attempts when connection is lost. The maximum number of times CAS attempts to reconnect to the Guardium system. Set this value to -1 for unlimited reconnection attempts. The default cas_max_reconnect_attempts and cas_reconnect_interval define an interval of about 3.5 days. After reaching the maximum, CAS continues to run, writing to the failover files, but it does not attempt to reconnect with a Guardium host.                                                                                                                                                                                                                             |
| Reconnect interval        | 60                | Wait time, in seconds, between reconnect attempts.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Raw data limit            | 1000              | Maximum number of KB written for an item when the Keep data checkbox is marked in the item template. If you specify -1, the size is unlimited.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Md5 data limit            | 1000              | Maximum size of a data item, KB, on which the MD5 checksum calculation is performed. If you specify -1, there is no limit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Linux-UNIX: S-TAP Control: Application server user identification parameters

These parameters affect the behavior of the S-TAP when an application user name needs to be bounded with database activities.

For more information, see [Linux-UNIX: Application server S-TAP configuration](#).

| Name               | Default value | Description                                                                                                                                                                                                                        |
|--------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Session timeout    |               |                                                                                                                                                                                                                                    |
| Ports              | 8080          | Comma-separated list of ports, or hyphens for inclusive ranges of ports, on which the Java™ application is accessed by a web browser.                                                                                              |
| Login pattern      |               | Comma-separated list of strings specifying the login pattern that is passed to the application. This pattern is passed to the Java application to identify a user login.                                                           |
| Username prefix    |               | Comma-separated list of strings specifying the prefix to the username for a specific session. This is the pattern the Java application uses to indicate the username of the given session.                                         |
| Username postfix   |               | Comma-separated list of strings specifying the postfix to the username for a specific session. This pattern is passed to the Java application to indicate the end of the value for the given variable that indicates the username. |
| Session pattern    |               | Comma-separated list of strings specifying the start of an end-user session, using a particular database session. This pattern specifies the [change of] end-user session for a specific database connection.                      |
| Session prefix     |               | Comma-separated list of strings specifying the session identifier.                                                                                                                                                                 |
| Session postfix    |               | Comma-separated list of strings specifying where the session ends.                                                                                                                                                                 |
| Session ID pattern |               | Comma-separated list of strings specifying the identifier for marking which end-user session a specific connection is continuing with.                                                                                             |
| Session ID prefix  |               | Comma-separated list of strings specifying what identifies or precedes the session_id in a specific users indicator packet.                                                                                                        |
| Session ID postfix |               | Comma-separated list of strings specifying where the session ID ends.                                                                                                                                                              |

## Linux-UNIX: S-TAP Control: Guardium Hosts parameters

These parameters describe a Guardium system to which this S-TAP can connect.

| Name          | Default value | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Guardium Host |               | IP address or hostname of the Guardium system that acts as the host for the S-TAP. You can add Guardium systems for failover or load balancing..                                                                                                                                                                                                                                                                                                                                                                   |
| Main threads  | 1             | The number of threads that are used between the S-TAP and a Guardium® host.<br>Valid values: 1-10 (maximum total of 10 for all defined Guardium hosts)<br>Note: Enterprise load balancing does not support multiple threads for a single managed unit. Set this parameter to 1 if you are using enterprise load balancing.                                                                                                                                                                                         |
| Pool Size     |               | The number of connections to open between the S-TAP and the sniffer process on a Guardium host. Increasing the value provides more throughput that might be required when encryption such as TLS is enabled. The maximum number of pooled connections is 50. The total is the sum of (connection_pool_size x num_main_thread) in all of the [SQLGuard_n] sections in the guard_tap.ini. Valid values: <ul style="list-style-type: none"><li>• 0: Disable pooling</li><li>• 1-10: (for each defined host)</li></ul> |
| Active        |               | <ul style="list-style-type: none"><li>• <input checked="" type="checkbox"/> connection is active.</li><li>• <input type="checkbox"/> connection is not active.</li></ul> <p>You can change the primary S-TAP by clicking Modify, and opening the Guardium Hosts section.</p>                                                                                                                                                                                                                                       |

## Related concepts

- [Linux-UNIX: Multi-threading S-TAP to increase S-TAP throughput](#)
- [Linux-UNIX: S-TAP load-balancing models and configuration guidelines](#)

## Linux-UNIX: S-TAP Control: Firewall parameters

These parameters affect the behavior of the S-TAP with respect to the firewall.

| Name                   | Default value                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Firewall installed     |                                     | Firewall feature enabled. Valid values: <ul style="list-style-type: none"><li>• <input type="checkbox"/> disabled.</li><li>• <input checked="" type="checkbox"/> enabled.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Firewall timeout       | 2                                   | Time, in seconds, to wait for a verdict from the Guardium® system. If the firewall times out, the value of the parameter Firewall fail close determines whether to block or allow the connection.<br>Valid values: 0-10.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Firewall default state | 0                                   | Valid values: <ul style="list-style-type: none"><li>• 0: Firewall is activated per session when triggered by a rule in the installed policy.</li><li>• 1: All traffic is watched for firewall policy violations</li><li>• 2: All traffic is watched for firewall policy violations for the initial priority_count packets (guard_tap.ini parameter). S-TAP watches the initial part of every new session to your DB. This is useful when you have session based policies, firewall rules based on the user, or some other information that is passed early in the session. It limits the impact of firewall on the performance. Instead of watching every bit of the session (Firewall default state=1) and waiting for an UNWATCH verdict, S-TAP simply unwatches automatically if no WATCH or DROP is sent.</li></ul> |
| Firewall fail close    | <input checked="" type="checkbox"/> | The action when the verdict cannot be set by the policy rules, for example the Firewall timeout expires. Valid values: <ul style="list-style-type: none"><li>• <input type="checkbox"/> the connection goes through.</li><li>• <input checked="" type="checkbox"/> the connection is blocked.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Firewall force watch   |                                     | When Firewall default state, then Firewall force watch specifies the network/mask of the IPs you want the firewall to watch, overriding the default (off).<br>Valid value: comma separated list of IP/mask values.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Firewall force unwatch |                                     | When Firewall default state=1 (on), then Firewall force unwatch specifies the network/mask of the IPs you want the firewall to ignore, overriding the default (on).<br>Valid value: comma separated list of IP/mask values.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Linux-UNIX: S-TAP Control: Inspection engine parameters

These parameters affect the behavior of the inspection engine that the S-TAP uses to monitor a data repository on a DB server. You can define up to 50 inspection engines per S-TAP.

| Name | Default value | Description |
|------|---------------|-------------|
|      |               |             |

| Name                     | Default value | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protocol                 |               | Required. The type of data repository that is monitored.<br>ASTERDB, Cassandra, CockroachDB, CouchDB, DB2®, Db2 Exit, ElasticSearch, exclude IE, FTP, GreenplumDB, HADOOP, HIVE, HP-Vertica, HTTP, HUE, IMPALA, Informix®, Informix Exit, KERBEROS, MariaDB, MemSQL, MongoDB, MySql, Netezza®, Oracle, PostgreSQL, REDIS, SAP Hana, Sybase, Teradata, Teradata Exit, WebHDFS, Windows File Share<br>If Protocol is one of the Exit libraries, only DB Install Dir and Intercept Types are needed.                                                                                                                                                                                                                                             |
| Port range               |               | For monitoring network traffic only, the port range over which to listen for database traffic. For a Kerberos inspection engine, set the start and end values to 88-88. If a range is used, do not include extra ports in the range, as this might result in excessive resource consumption while the S-TAP attempts to analyze unwanted traffic.<br>Examples:<br>To monitor range 1521-1525 (5 ports) with no port forwarding: <ul style="list-style-type: none"> <li>• Port range = 1521-1525</li> <li>• DB Real Port =1521</li> </ul> To monitor range 2000-2004 (5 ports) where network port 2000 is mapped to local port 1521: <ul style="list-style-type: none"> <li>• Port range = 2000-2004</li> <li>• DB Real Port = 1521</li> </ul> |
| DB Real Port             | 4100          | With K-TAP and PCAP, identifies the database port or range of ports to be monitored. For exit libraries, use its value for db_home.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Client Ip/Mask           |               | Restricts S-TAP to monitor traffic only from the specified sets of IP address and mask pairs, by using a list of addresses in IP address/mask format: n.n.n.n/m.m.m.m. If an improper IP address/mask is entered, the S-TAP does not start. Valid values: <ul style="list-style-type: none"> <li>• User-defined list</li> <li>• 0.0.0.0/0.0.0.0::/0: select all clients.</li> <li>• 127.0.0.1/255.255.255.255::1/0: local traffic only</li> </ul> Client Ip/Mask (networks) and Exclude Client Ip/Mask (exclude networks) cannot be specified simultaneously.<br>If the value of this parameter is not configured correctly, the value is replaced by the default value.                                                                      |
| Exclude Client Ip/Mask   |               | A list of client IP addresses and corresponding masks that are excluded from monitoring. Use this option to configure the S-TAP to monitor all clients, except for a certain client or subnet (or a collection thereof). Client Ip/Mask (networks) and Exclude Client Ip/Mask (exclude networks) cannot be specified simultaneously.                                                                                                                                                                                                                                                                                                                                                                                                          |
| Connect To Ip            | 127.0.0.1::1  | IP address for S-TAP to use to connect to the database. When K-TAP is enabled, this parameter is used for Solaris Zones and AIX WPARs and it should be the zone IP address in order to capture traffic.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| DB User                  | NULL          | OS username (case-sensitive) of the owner of the DB server process (for example, oracle). This parameter specifies which user is allowed to use the db_request_handler socket. It is required if you are not using the user root. If set to an invalid value, A-TAP cannot access the socket to retrieve permission for accessing K-TAP. In this case, it requires authorization with a group membership to log decrypted traffic to K-TAP (by using the guardctl <b>authorize-user</b> command). You can define a comma-separated string of multiple users.                                                                                                                                                                                  |
| DB Install Dir           | NULL          | Db2, Informix, and Oracle: Enter the full path name for the database installation directory. For example: /home/oracle10. All other database types enter: NULL. For Db2 exit and Informix exit, db_install_dir must be exactly the same as the \$HOME value in the database (or \$DB2_HOME for Db2 Exit); otherwise tap_identifier does not function properly.                                                                                                                                                                                                                                                                                                                                                                                |
| Process Name             | NULL          | The value of this parameter depends on whether it's in an exit, and whether there is A-TAP. <ul style="list-style-type: none"> <li>• Exit libraries: see <a href="#">Linux-UNIX: Configuring Exit libraries</a></li> <li>• With A-TAP: see <a href="#">Linux-UNIX: Database-specific guardctl parameters</a></li> <li>• Without A-TAP: The full path name for the database executable. For example: <ul style="list-style-type: none"> <li>◦ Oracle: /\$ORACLE_HOME/bin/oracle</li> <li>◦ Informix: /INFORMIXTMP/.inf.sqlexec. Applies to all Informix platforms but Linux®.</li> <li>◦ Informix with Linux, example: /home/informix11/bin/oninit</li> <li>◦ MYSQL: mysql</li> </ul> </li> </ul>                                              |
| DB2 Shared Mem. Adjust   | 20            | Required when Db2® is selected as the database type, and shared memory connections are monitored. The offset to the server's portion of the shared memory area. Offset to the beginning of the Db2 shared memory packet, depends on the Db2 version: 32 in pre-8.2.1, and 80 in 8.2.1 and higher.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| DB2 Sh. Mem. Client pos. | 61440         | The offset to the client's portion of the shared memory area. Required when Db2 is selected as the database type, and shared memory connections are monitored. Use the script find_db2_shmem_parameters.sh to find the value. The script is located in stap_directory/bin, and outputs what the Db2 shared memory parameters that are defined in the Inspection Engines should be. Run it either as root or Db2 user, by using the syntax: find_db2_shmem_parameters.sh <instance name>. You can run it from any directory.                                                                                                                                                                                                                   |
| DB2 Shared Mem. Size     | 131072        | Db2 shared memory segment size. Required when Db2 is selected as the database type, and shared memory connections are monitored.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Name               | Default value | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Encryption         | 0             | <p>Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Unencrypted</li> <li>• 1: Encrypted</li> </ul> <p>Default = 0 (false)<br/>Activate ASO or SSL encrypted traffic for Oracle (versions 11 and 12) and Sybase on Solaris, HPUX, and AIX®.</p> <p>For Oracle, specify db_version in the guard_tap.ini file (for example, db_version=12)</p> <p>For Oracle12 SSL, instrument on all platforms. For Oracle11 SSL, instrument on AIX.</p> <p>For any Oracle requiring instrumentation, if you are using encryption=1 in the guard_tap.ini (which is not supported on Linux), you must instrument before setting that parameter.</p> <p>Some DBs require restart after enabling encryption.</p> <p>When using GIM to configure the S-TAP, GIM_ROOT_DIR must be set to the absolute path to the modules, for example /usr/local/guardium/modules</p> |
| Intercept Types    | NULL          | DO NOT change this parameter unless it is absolutely necessary. Protocol types that are intercepted by the IE. Valid values: <ul style="list-style-type: none"> <li>• NULL: auto intercepts all protocols the Database supports</li> <li>• Comma-separated list: IE intercepts these protocol types only.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Identifier         | NULL          | Used to distinguish inspection engines from one another. If unspecified, Guardium® auto-populates the field with a unique name that uses the database type and sequence number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| DB Version         | 9             | The database version. The string must start with a numeral and not a letter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Unix Socket Marker | Null          | Specifies UNIX domain sockets marker for Oracle, MySQL, and Postgres. Usually the default is correct, but when the named pipe or UNIX domain socket traffic does not work then you need to make sure that this value is set correctly. For example, for Oracle, set unix_domain_socket_marker to the KEY of IPC defined in tnsnames.ora. If it is NULL or not set, the S-TAP uses defined default markers identified as: * MySQL - "mysql.sock" * Oracle - "./oracle/" * Postgres - ".s.PGSQL.5432"                                                                                                                                                                                                                                                                                                                                                          |

## Linux-UNIX: Scheduling S-TAP diagnostics

12.1 and later You can schedule S-TAP diagnostics by using the S-TAP Diagnostic Scheduler user interface.

### Before you begin

You must be logged in to the Guardium system that is the active host for the S-TAP®.

### Procedure

1. Browse to [Manage > Activity Monitoring > S-TAP Diagnostic Scheduler](#).  
You can see all the UNIX S-TAP hosts that are listed under the S-TAP Hosts column that are managed by the Guardium system. This is the same list that is present on the S-TAP Control page.
2. Select one or more S-TAP hosts and click Add to schedule. The following options are available to run the diagnostics:
  - Click Create Schedule to create a schedule to run the diagnostics and enter the details.
  - Click Run Once to run the diagnostic immediately.  
Important: After you run the diagnostics, click refresh to view the diagnostic results in the grid.
3. To remove the S-TAP hosts from the diagnostic schedule, select one or more S-TAP hosts from the S-TAP Hosts list and click Remove from schedule.
4. Optional: Click edit icon to edit the following S-TAP host details:
  - Participate in scheduled diagnostics
  - Level
  - Duration

## Linux-UNIX: Configure S-TAP with guard-config-update

You can use the guard-config-update script to update your S-TAP configuration (without using the GUI), whether S-TAP was installed with GIM, RPM, or shell.

### About this task

### Procedure

1. Log in to the database server as `root` and change the directory to `/opt/guardium`.
2. Run the script `guard-config-update` using the relevant options and actions from this list:

Table 1. guard-config update parameters

| Parameter  | Description                                                            |
|------------|------------------------------------------------------------------------|
| --stap-dir | S-TAP install directory if not default (default: /usr/local/guardium). |

| Parameter                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| --migrate-to-insights [tenant ID] [routeName] | Migrate an S-TAP to Guardium® Insights. Parameters:<br><br>tenant ID<br>The Guardium Insights tenant ID, including the <i>TNT_</i> prefix.<br>routeName<br>The DNS hostname for the Guardium Insights deployment. The DNS hostname is the same as the URL for the UI (without the https:// prefix).<br><br>Note: Before migrating the S-TAP, Guardium Insights must have a signed, trusted certificate that the S-TAP can locate. Store the certificate either in the default location ( <code>INSTALL_DIR/etc/pki/certs/trusted/ca.cert.pem</code> , where <code>INSTALL_DIR</code> is the Guardium Data Protection installation directory or configure a different location in the <code>guard_tap.ini</code> by using the <code>guardium_ca_path</code> parameter. If you specify a custom location, you must manually store the certificate (that is, you cannot use the <a href="#">push_insights_trust API</a> ).<br>You can also use the <a href="#">migrate_stap_config API</a> to migrate S-TAPS. |
| --set-tap-ip [IP or hostname]                 | Set <code>tap_ip</code> in S-TAP config file <code>/usr/local/guardium/guard_stap/guard_tap.ini</code> (default: <code>rh5u9x64t.guard.swg.usma.ibm.com</code> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| --set-sqlguard-ip [IP or hostname]            | Set <code>sqlguard_ip</code> in SQLGuard_0 section in S-TAP config file <code>/usr/local/guardium/guard_stap/guard_tap.ini</code> (default: <code>127.0.0.1</code> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| --add-sqlguard-[ID] [IP or hostname]          | Add SQLGuard_ID section to S-TAP config file <code>/usr/local/guardium/guard_stap/guard_tap.ini</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| --remove-sqlguard [ID]                        | Remove SQLGuard_ID section from the S-TAP config file <code>/usr/local/guardium/guard_stap/guard_tap.ini</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| --modify-sqlguard [ID] [parameter] [value]    | Set SQLGuard_ID section parameter to value in S-TAP config file <code>/usr/local/guardium/guard_stap/guard_tap.ini</code> . Parameters:<br><br><code>sqlguard_ip</code><br>IP address or hostname of SQLGuard unit<br><code>sqlguard_port</code><br>Port used to connect to SQLGuard unit (default: 16016)<br><code>primary</code><br>Order of preference (1=primary, 2=secondary, 3=tertiary, and so on)<br><code>num_main_thread</code><br>Number of main connections to use for this SQLGuard, used with <code>participate_in_load_balancing = { 1, 4 }</code> (default: 1)<br><code>connection_pool_size</code><br>Number of data connections per main connection to SQLGuard unit (default: 0)                                                                                                                                                                                                                                                                                                        |
| --modify-tap [parameter] [value]              | Set TAP section parameter to value in S-TAP config file <code>/usr/local/guardium/guard_stap/guard_tap.ini</code> . For the list of <code>guard_tap.ini</code> parameters, see <a href="#">guard_tap.ini parameters</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| --help-config [option]                        | Show information about an option in the ini, if available (show all available if none specified).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| --set-flexload [0 or 1]                       | Controls the K-TAP FlexLoad mechanism: 0: disable, 1: enable.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| --retry-ktap-load                             | Retry K-TAP loading (useful after installing dev packages, updating after K-TAP request, or changing flexload; automatically restarts S-TAP).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| --discover-ies                                | Run discovery and replace all Inspection Engines with those discovered.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| --stop [service]                              | Stop service (S-TAP, or monitor) temporarily (Solaris services and inittab treat this as permanent disable, does not auto-start on boot until re-enabled).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| --start [service]                             | Start service (S-TAP, or monitor) if not already running (implies enable).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| --restart [service]                           | Restart service (S-TAP, or monitor) if already running.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| --disable [service]                           | Prevent service (S-TAP, or monitor) from running again.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| --enable [service]                            | Configure service (S-TAP, or monitor) for automatic start.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| --status                                      | Show which services are started and if they are configured to start automatically.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| --show-tap [option]                           | Shows the value that is currently stored for a parameter in the TAP section of the <code>guard_tap.ini</code> file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| --show-ies                                    | Shows the currently configured inspection engines in the <code>guard_tap.ini</code> file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| --set-ktap-prevent-exact-match-build          | Enable or disable the K-TAP local build. It is recommended to leave the KTAP local build enabled, which is the default setting when installing.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

3. Restart the S-TAP. For example, `/opt/guardium/guard_stap/guard-config-update --restart stap`.

## Linux-UNIX: Discover database instances

Enable S-TAP to periodically discover database instances and send the results to the current active S-TAP system.

The Guardium® Discovery Agent is a software agent that is automatically installed with the S-TAP package on a database server. The instance discovery agent reports database instances, listener, and port information to the Guardium system. Discovery does not find and report on every detail of the database instances on the server.

Auto-discovery is enabled by default during installation. It runs once daily. When discovery runs, it identifies the user modifications in the `guard_tap.ini`, and does not overwrite them with the discovered database details.

Guardium recommends that you leave the parameter values at their defaults. The parameters are described in [Linux-UNIX: Discovery parameters](#).

Database types that are supported by S-TAP discovery are listed in the [Guardium support matrix](#).

You can define rules to manage inspection engine creation on discovered databases. For more information, see [Database discovered instances rules](#).

The discovery bundle is not installed in a worker zone or WPAR; the discovery agent that is running on the global zone collects information from other zones. Limitation: On Solaris zones architecture, when Db2 instances are running on worker zones, Discovery does not discover the Db2 shared memory parameters.

Newly discovered database instances can be seen in the Discovered Instances report. From this report, datasources and inspection engines can quickly be added to Guardium using the Actions menu.

If databases on the database server are not operational (started) or are added later, the Discovery Agent can still discover these instances. Go to [Manage > Activity Monitoring > S-TAP Control](#), click , and select Run Database Instance Discovery.

S-TAP Discovery can be run manually but this action is not suggested. The main reason to run it manually is for debugging purposes. If a new request comes in from the user interface while a scheduled discovery is running, the new request is ignored.

Note: Once you activate A-TAP, you no longer need to run the S-TAP Discovery instance as it is already replaced by A-TAP.

You can run Discovery from a local command line on the database server (`/usr/local/guardium/guard_stap/guard_discovery`) by using one of these flags:

- `--update-tap` flag: edits the `guard_tap.ini` to add or update inspection engines
- `--send-to-sqlguard` flag (or with no flag, which is the default): sends the found changes to the Guardium system, where they appear in the Discovered Instances report
- `--print-output` flag: prints the found changes to `stdout` (for debugging)

If the S-TAP is running as "user" (and not guardium), the discovery functionality is limited. The following message displays:

WARNING: Discovery is enabled and STAP is running as user guardium.  
The discovery function is limited when STAP runs as user guardium.  
Discovery is most effective when '`tap_run_as_root=1`'

Note: To avoid an instance where S-TAP discovery does not open the Informix database, it is recommended to start Informix databases by using the full path to the executable.

Discovery also uses these parameters:

- `tap_ip`: the S-TAP with which the database instance is associated.
- `sqlguard_ip`: S-TAP discovery results are sent to this IP. (The Guardium system with `primary=1` in the SQLguard parameters.)

## Using Exit discovery

The Exit discovery feature allows database auto-discovery to discover any databases that have Exit protocols and add those instances to Discovered Instances report. By default, Exit discovery is disabled.

Guardium provides several ways to enable or disable Exit discovery.

- From the S-TAP Configuration page in the Guardium GUI - Select or clear Use exit db type to enable or disable Exit discovery .
- From GIM - To enable Exit discovery, set the `STAP_USE_EXIT_DB_TYPE` GIM parameter to 1. When `STAP_USE_EXIT_DB_TYPE` GIM is enabled, set `KTAP_ENABLED=0` to disable KTAP.  
To disable Exit discovery, set `STAP_USE_EXIT_DB_TYPE` GIM=0 (the default).
- By using the `update_stap_config` GuardAPI or REST API - For example, to enable Exit discovery for Informix, use the following command:  
`grdapic update_stap_config stapHost=2.2.2.2 updateValue=TAP.USCE_EXIT_DB_TYPE:1,TAP.DB_EXIT_LIST:Informix`

Setting up Exit discovery:

- When you install an S-TAP, you can set the `STAP_USE_EXIT_DB_TYPE` parameter to 1. In this case, K-TAP is disabled and Guardium discovers the Exit inspection engine and adds it to `guard_tap.ini` file as `use_exit_db_type=1`.
- You can also update an existing S-TAP to use Exit discovery. Update the S-TAP configuration through the GIM GUI to set `STAP_USE_EXIT_DB_TYPE` to 1.
- When `STAP_USE_EXIT_DB_TYPE` is set to 1, you can also set `STAP_DB_EXIT_LIST` to specify which database Exits to discover. For more information, see [STAP DB EXIT LIST](#) in [Linux-UNIX: General parameters](#).

You can also run discovery from the S-TAP control page in the UI, which updates the inspection engine immediately if the Replace Inspection Engines box is selected. For more information, see [Linux-UNIX: Configuring S-TAP in the S-TAP Control page](#).

Note: When Exit discovery is on, you can monitor only databases that support Exit protocols.

## Linux-UNIX: Configuring an Inspection Engine

Configure or modify an inspection engine in the S-TAP Control pane.

### Before you begin

You must be logged in to the Guardium system that manages the S-TAP.

### About this task

Do not configure an S-TAP inspection engine to monitor network traffic that is also monitored directly by a Guardium system that is hosting the S-TAP, or by another S-TAP reporting to the same Guardium system. That would cause the Guardium system to receive duplicate information: it would not be able to reconstruct sessions, and it would ignore that traffic.

You can also add inspection engines directly in the `guard_tap.ini` file, see [Linux-UNIX: Editing the S-TAP configuration parameters](#).

You can define up to 50 inspection engines per S-TAP.

## Procedure

---

1. Navigate to `Manage > Activity Monitoring > S-TAP Control`.
2. In the row of the S-TAP, click .  
The S-TAP Configuration window opens.
3. Scroll to the bottom of the inspection engines, and click next to Add Inspection Engine....  
Note: You can add a maximum of 50 Inspection Engines only. If you exceed this limit, then the additional engines are truncated.
4. Select the protocol and enter the port range. The window refreshes with the relevant parameters, some with their default values.
5. Configure all the required parameters, and click Add. If you are missing parameters, the system informs you what is missing.

## Related tasks

---

- [Linux-UNIX: S-TAP configuration per database type](#)

## Related reference

---

- [Linux-UNIX: Inspection engine parameters](#)

## Linux-UNIX: Inspection engine verification

---

S-TAP verification confirms that the S-TAPs and their inspection engines in your environment are running and actively monitoring database activity. Understand verification, and define a schedule to regularly verify S-TAPs.

Verification checks the sniffer operation and communication between the Guardium system and the inspection engines. You can enable verification for all S-TAP clients on your system, or individual S-TAP clients, or individual inspection engines.

Verification is supported for these database types:

- Db2
- Greenplum
- Informix
- MSSQL (for cluster configuration supports only advanced verification)
- MySQL
- Netezza
- Oracle
- PostgreSQL
- Teradata (advanced verification only)

There are two types of verification:

### Standard verification

Checks the sniffer operation, and the communication between the S-TAP and the inspection engine. During standard verification, Guardium® attempts to log in to database defined in the inspection engine with user `resutlfd`, based on the assumption that no such user exists on the target system. (If that user exists, use advanced verification instead.) Depending on the installed policy, failed login alerts might be triggered for that login attempt. Next, the verification process checks whether it can connect to the selected inspection engine on the database server. It expects to receive a response that indicates a failed login. If a different response is received, you might have to investigate further.

Some error messages from individual databases do not indicate a specific problem. For example, on several supported databases, the error code that is returned for a wrong port can also mean that the database itself is not started.

### Advanced verification

Use advanced verification to avoid failed login requests, and manage individual inspection engines. During advanced verification, Guardium logs into the database that is defined in the configured datasource. It runs `select * from non_existent_table`. Depending on the installed policy, this SQL might appear in reports or alerts.

- [Linux-UNIX: S-TAP verification](#)

The S-TAP verification process checks several configuration parameters and attempts to connect to the inspection engines.

- [Linux-UNIX: Configure standard verification](#)

Use this task to add all inspection engines on a specific S-TAP client host to the verification schedule.

- [Linux-UNIX: Configure advanced verification](#)

Use this task to run advanced verification on individual inspection engines on a specific S-TAP client host, and to add individual inspection engines to advanced verification.

- [Linux-UNIX: Configuring the S-TAP verification schedule](#)

The default schedule for verifying S-TAPs is once per hour, every day. You can change this schedule.

---

## Linux-UNIX: S-TAP verification

The S-TAP verification process checks several configuration parameters and attempts to connect to the inspection engines.

Before connecting to the database, the verification process checks whether the sniffer process is running on the Guardium® system. The sniffer is responsible for communicating with each S-TAP and processing the data that is received. If the sniffer is not running, responses from the S-TAP are not recognized.

The verification process attempts to log in to your database's STAP client with an erroneous user ID and password, to verify that this attempt is recognized and communicated to the Guardium system.

Next the verification process checks whether it can connect to the selected inspection engine on the database server. It expects to receive a response that indicates a failed login. If a different response is received, you might have to investigate further.

Some error messages from individual databases do not indicate a specific problem. For example, on several supported databases, the error code returned for a wrong port can also mean that the database itself is not started.

## Linux-UNIX: Configure standard verification

Use this task to add all inspection engines on a specific S-TAP client host to the verification schedule.

### About this task

As an alternative to this procedure, you can:

- use the GRDAPI command `verify_stap_inspection_engine_with_sequence`.
- Use the procedure in [Linux-UNIX: Configure advanced verification](#) to configure verification on individual inspection engines, by clicking Verify in step 3. The system immediately outputs results. Failed checks are shown first, with recommendations for next steps. Checks that succeeded are shown in a collapsed section at the end of the list. In some situations, it might be useful to review the successful checks in order to choose among possible next steps.

### Procedure

- Access [Manage > Activity Monitoring > S-TAP Control](#).
- Use these options:
  - Add All to Schedule: add all inspection engines for all displayed S-TAPs to verification.
  - Remove All from Schedule: remove all inspection engines for all displayed S-TAPs from verification.
  - Add to Schedule: add all inspection engines of the selected S-TAP client to the schedule.
- If an S-TAP does not have the option All Can Control enabled, you can only change its status if your Guardium system is the primary system for this S-TAP.
- Click Refresh.
- To verify now, go to [Manage > Activity Monitoring > S-TAP Verification Scheduler](#) and click Run Once Now.
- By default, the system waits five seconds before displaying verification results. If your network latency is high, this might not be enough time to receive the expected response from the database server. If you need to allow more time, you can use the `store stap network_latency` CLI command to change the period.

### What to do next

View the verification results in the S-TAP Verification page ([Manage > Reports > Activity Monitoring > S-TAP Verification](#) page).

## Linux-UNIX: Configure advanced verification

Use this task to run advanced verification on individual inspection engines on a specific S-TAP client host, and to add individual inspection engines to advanced verification.

### Procedure

- Access [Manage > System View > S-TAP Status Monitor](#).
- Click anywhere in the row of the S-TAP.  
The window refreshes with the individual inspection engines of this host.
- To output immediate verification results, take the following steps:
  - Click one inspection engine, and click Advanced Verify.
  - 12.0 Optionally, under Datasource, select Show only matching S-TAP host or select a name from the Name list to search for a specific inspection engine.  
12.1 and later Optionally, under Datasource, make sure that Show only matching S-TAP host and host is selected. If you select a datasource for which the IP address or port does not match the datasource, then an error message is returned.
  - Click Verify.
- The S-TAP Verification Results opens. Failed checks are shown first, with recommendations for next steps. Checks that succeeded are shown in a collapsed section at the end of the list. In some situations, it might be useful to review the successful checks in order to choose among possible next steps.
- By default, the system waits five seconds before it displays verification results. If your network latency is high, five seconds might not be enough time to receive the expected response from the database server. If you need to allow more time, you can use the `store stap network_latency` CLI command to change the period.
- To add to or remove individual inspection engines to the verification schedule:
  - Select one or more inspection engines.
  - Click Add to Schedule or Remove from Schedule

### What to do next

View the results of schedules verification in the S-TAP Verification page ([Manage > Reports > Activity Monitoring > S-TAP Verification](#)).

## Linux-UNIX: Configuring the S-TAP verification schedule

The default schedule for verifying S-TAPs is once per hour, every day. You can change this schedule.

### About this task

The same schedule is used for all S-TAPs that are scheduled for verification.

Once a schedule is defined, you can click the Pause button in the S-TAP Verification Scheduler to temporarily stop the verification process while keeping it active. Use the Run Once Now button to run the verification once in real-time.

### Procedure

1. Click [Manage > Activity Monitoring > S-TAP Verification Scheduler](#) to open the S-TAP Verification Scheduler.
2. In the S-TAP Verification Scheduler portion of the page, click [Modify Schedule](#).
3. In the Schedule Definition dialog, use the drop-down lists and check boxes to schedule when verification runs.  
This schedule is applied to all S-TAPs that are scheduled for verification.
4. Click [Save](#) to save your changes.

## Linux-UNIX: S-TAP load-balancing models and configuration guidelines

Understand the S-TAP load-balancing models, and choose the one appropriate to your setup.

The two main reasons for using load balancing:

- To improve reliability. If one collector fails, the traffic is rerouted to another collector so that no traffic is lost.
- To increase throughput. Load-balancing shares your high-volume traffic between a few collectors.

### Failover

S-TAP sends traffic to one collector (primary) and fails over to one or more collectors (secondary, tertiary, and so on) as needed. The S-TAP agents are configured with a primary and at least one secondary collector IP. If the S-TAP agent cannot send the traffic to the primary collector, the S-TAP agent automatically fails over to the secondary. It continues to send data to the secondary host until either the secondary host system becomes unavailable, the primary host becomes available again, or until the S-TAP is restarted (at which point it attempts to connect to its primary host first). If the secondary host system becomes unavailable, it fails over to the tertiary if there is one defined. In the second case S-TAP fails over from the secondary Guardium® host back to the primary Guardium host.

Set up a primary and up to two secondary collectors. You can either define one collector as a standby failover collector only, or a few failover collectors. When you use one standby failover, one collector is usually sufficient for 4-5 collectors. When you use a few failover collectors, each one should run at a maximum 50% capacity, so that there are always resources for extra load. Choose the setup that works best with your architecture, database, and data center layout.

The S-TAP restarts each time configuration changes are applied from the active host.

1. In the S-TAP Control window, Details section: set Load balancing to 0; In the Guardium Hosts section: add at least one secondary Guardium Host.

Note: If you are not an advanced user, do not update the default failover configuration default values.

2. Before you designate a Guardium system as a secondary host for an S-TAP, verify these items.

- The Guardium system must have connectivity to the database server where S-TAP is installed. When multiple Guardium systems are used, they are often attached to disjointed branches of the network.
- The Guardium system must not have a security policy that will ignore session data from the database server where S-TAP is installed. In many cases, a Guardium security policy is built to focus on a narrow subset of the observable database traffic, ignoring all other sessions. Make sure that the secondary host will not ignore session data from S-TAP or modify the security policy on the Guardium system as necessary.

#### Enhanced failover mechanism to avoid data loss

12.1 and later

The main goal of failover mechanism is to preserve the session parameters when switching the S-TAP to the secondary collector. The regular failover mechanism saves session parameters as 'failover messages' that are received from the primary collector over the network. If a failover occurs, the mechanism forwards the failover messages to the secondary collector. In rare cases, the failover messages are lost. To address this, the enhanced failover mechanism, also saves session parameters in the form of several raw database protocol packets. If a failover is required and the failover messages are lost, the failover mechanism forwards the raw database packets to the secondary collector.

### Load balancing

This configuration balances traffic from one database onto multiple collectors based on the client ports. This option is useful when you must monitor all traffic (comprehensive monitoring) of an active database. (Note that for outliers detection, the collectors must be under the same aggregator and central manager so that the aggregator can process all related data.) When the generated traffic is large and you need to house the data online on a collector for an extended period, use this method because it performs session-based load balancing across multiple collectors. An S-TAP can be configured in this manner with up to 10 collectors.

Complete the following configuration procedure in the Details section of the S-TAP Control window.

- Set the Value of the Load balancing parameter to 1 for load balancing.

### Internal load balancing

12.1 and later

The Internal Load Balancer (ILB) helps avoid data loss caused due to collector overload.

The ILB evaluates the data load and helps avoid the data loss by proactively forecasting the load on the collector and redirecting the traffic to another collector to balance this load.

On the sniffer, ILB dynamically determines the number of sessions that a sniffer can accept from the S-TAP. This value is based on the collector's capacity for session information and processing collector load.

ILB sends two values to the S-TAP: the total number of allowed sessions on the appliance and the total number of sessions currently opened in the sniffer.

Note: The calculation of current sessions includes all the connected S-TAPs.

Each S-TAP keeps count of open sessions and uses the allowed session count to determine whether it can send new session data to the existing collector.

If number of open sessions is more than the allowed session count, then the S-TAP redirects new sessions to another collector.

If the number of open sessions do not exceed the allowed session count then the S-TAP may send the new sessions to existing collector.

## Enabling internal load balancer

---

12.1 and later

Enabling on UNIX

1. To enable the internal load balancer feature on S-TAP, set the INTERNAL\_LOAD\_BALANCER\_ENABLED parameter to 1. Default value = 0. Value range = 0, 1.
2. Also, set the PARTICIPATE\_IN\_LOAD\_BALANCING to 4.  
Default value = 0. Valid values = 0 - 4

Enabling on collector

1. Create a session-level policy. For more information on creating session-level policy, see [Creating session-level policies](#).
2. In the Rule action field, select CONFIGURE.
3. In the Option field, select ILB and click OK.

## Grid

---

With Grid, the S-TAP communicates to the collector through a load balancer, such as f5 and Cisco. The S-TAP agent is configured to send traffic to the load balancer. The load balancer forwards the S-TAP traffic to one of the collectors in the pool of collectors. You also can configure failover between load balancers for continuous monitoring if the load balancer should fail.

S-TAP attempts to write to the buffer at an interval of tap\_min\_heartbeat\_interval. If it fails 5 times consecutively it fails over. Also, if it detects that the buffer is half full, it fails over.

1. In the Details section of the S-TAP Control window, set the value of the Load balancing parameter to 3 for the grid model. For more information, see [S-TAP Control: Details](#).
2. Set all can control = 1.
3. Guardium Host = <the IP of the Virtual IP of the balancer, to which all S-TAP database clients point to>.

## Redundancy

---

In redundancy, the S-TAP communicates its entire payload to multiple collectors. The S-TAP is configured with more than one collector (often only two) and communicates the identical content to both. This option provides full redundancy of the same logged data across multiple collectors. It can also be used for logging data and alert on activity at different levels of granularity.

In the Details section of the S-TAP Control window, set the value of the Load balancing parameter to 2 for redundancy. For more information, see [S-TAP Control: Details](#).

### Multiple K-TAP buffers

This mode works the same as when Load balancing is set to 1 but utilizes extra threads and K-TAP buffers to increase throughput. In the Details section of the S-TAP Control window, set the value of the Load balancing parameter to 4. See [Linux-UNIX: Multi-threading S-TAP to increase S-TAP throughput](#).

Note: If there is no K-TAP being used and Load balancing is set to 4, the behavior is the same as with Load balancing set to 1.

## Linux-UNIX: Kerberos-authenticated database traffic

---

Kerberos is a network authentication protocol that eliminates the transmission of unencrypted passwords across the network.

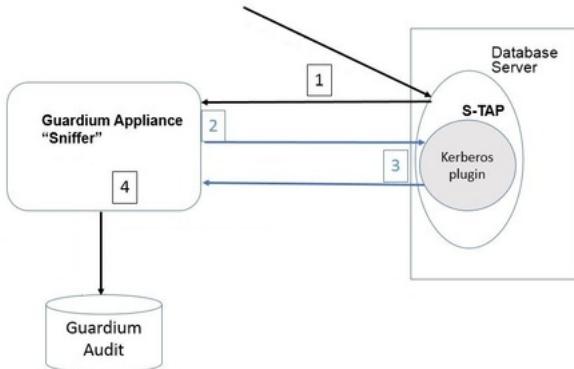
It works in a mutual authentication mode, verifying both the identity of the user that is requesting authentication as well as the server providing the requested authentication. The Kerberos authentication mechanism issues tickets for accessing network services. These tickets contain encrypted data, including an encrypted password, that confirms the user's identity to the requested service.

For auditing and alerting, it's important to know which database user performed an action. When login is done with a Kerberos ticket, determining the database user is not always straightforward.

Guardium S-TAP only sees network traffic and passes it on to the sniffer on the Guardium appliance. When a Kerberos ticket is used for login, S-TAP passes that Kerberos ticket along to the sniffer. For some database server types, the sniffer can determine the database user from the Kerberos login traffic and no additional information is required. For other database server types, the sniffer needs some assistance. That function is performed by the S-TAP Kerberos plugin.

The S-TAP Kerberos plugin is not enabled by default; it requires additional configuration.

If you use Kerberos at all, configure the plugin. There is no performance implication or other downside to configuring the plugin, just in case you need it.



The data flow between the database, the Guardium® sniffer and the Guardium audit data is:

1. S-TAP captures the Kerberized database login packet (along with other activity) and sends it to the Guardium appliance.
2. If the sniffer can determine the user name from the Kerberos ticket, it parses it.
3. If the sniffer cannot determine the user name from the Kerberos ticket, it sends the Kerberos ticket, along with a request for the database user, to the S-TAP. S-TAP checks to see if there is a Kerberos plugin configured. If there is a Kerberos plugin configured, S-TAP gives the ticket to the plugin and the plugin attempts to figure out DB\_USER from the ticket. It returns the database user name to S-TAP. (If not, then the database user name is not supplied and you do not see database user names in your reports.)
4. The sniffer can now populate the database user for that ticket, and correlate it with the rest of the database activity for that user in the Audit.

- [\*\*Linux-UNIX: Kerberos authentication supported databases\*\*](#)

View the list of database servers that are supported for Kerberos authentication, and whether they require the Kerberos plugin.

- [\*\*Linux-UNIX: Configuring Kerberos by using the setup\\_kerberos.sh script\*\*](#)

Run the setup\_kerberos.sh script to configure and activate Kerberos on your Oracle, Sybase and DB2 databases. The script makes all of the configuration updates in both the database and the S-TAP.

- [\*\*Linux-UNIX: Enabling the Kerberos plugin\*\*](#)

To enable the plugin, edit the guard\_tap.ini configuration file and change the **kerberos\_plugin\_dir** entry to point to the directory where the plugin itself (libguardkerbplugin.so) and the configuration file (guardkerbplugin.conf) are located.

- [\*\*Linux-UNIX: Configuring the Kerberos plugin\*\*](#)

To monitor database traffic on a server that uses Kerberos authentication, including identifying the DB\_USER, you must configure the guardtap.ini and guardkerbplugin.conf files appropriately.

- [\*\*Linux-UNIX: Finding the Kerberos configuration parameters for Oracle\*\*](#)

For Oracle Kerberos, locate the Kerberos keytab and configuration file locations in sqlnet.ora.

- [\*\*Linux-UNIX: Finding the Kerberos configuration parameters for Sybase\*\*](#)

Use the Sybase environment variables to get the Kerberos information.

- [\*\*Linux-UNIX: Merging keytab files\*\*](#)

If you have multiple keytab files (for multiple databases on one host), you can merge the keys. After combining the keytabs, configure the Kerberos plugin to point to the one new combined keytab. Each database continues to use its own individual keytab, not the combined one.

## Linux-UNIX: Kerberos authentication supported databases

View the list of database servers that are supported for Kerberos authentication, and whether they require the Kerberos plugin.

| Database   | Kerberos plugin required? |
|------------|---------------------------|
| Db2        | No                        |
| Oracle     | Yes                       |
| Cassandra  | Yes                       |
| Sybase ASE | Yes                       |
| HBase      | Yes                       |
| MongoDB    | No                        |
| HDFS       | No                        |
| Big SQL    | No                        |
| Hive       | Yes                       |
| Impala     | No                        |

## Linux-UNIX: Configuring Kerberos by using the setup\_kerberos.sh script

Run the setup\_kerberos.sh script to configure and activate Kerberos on your Oracle, Sybase and DB2 databases. The script makes all of the configuration updates in both the database and the S-TAP.

### Before you begin

- Make sure you know the database username.
- Inspection engines must be configured on the databases before you run the script because it scans the database environments.

### About this task

- The setup\_kerberos.sh script is part of the S-TAP installation, and is located in the S-TAP installation directory.
- This script is an alternative to the Kerberos configuration tasks described in [Linux-UNIX: Enabling the Kerberos plugin](#), [Linux-UNIX: Configuring the Kerberos plugin](#), [Linux-UNIX: Finding the Kerberos configuration parameters for Oracle](#), [Linux-UNIX: Finding the Kerberos configuration parameters for Sybase](#).
- The script has these flags:
  - d: disable plugin
  - e: enable plugin
  - s: scan
  - S: scan and update configuration
  - v: verbose
  - h: print this help

## Procedure

---

- Log in to the database server as `root`, and access the S-TAP installation directory.
  - To enable, scan the databases, and enable the configuration, run `setup_kerberos.sh -e enable plugin -s scan -S scan and update configuration`. The script starts to run, and prompts you for the required details.
  - When the script completes without errors, restart the S-TAP.
- 

## Linux-UNIX: Enabling the Kerberos plugin

To enable the plugin, edit the `guard_tap.ini` configuration file and change the `kerberos_plugin_dir` entry to point to the directory where the plugin itself (`libguardkerbplugin.so`) and the configuration file (`guardkerbplugin.conf`) are located.

## Procedure

---

- For a default shell install: `kerberos_plugin_dir=/usr/local/guardium/guard_stap`
  - For a default GIM install: (exact path varies with software release in use)  
`kerberos_plugin_dir=/usr/local/IBM/modules/STAP/current/10.1.3_r101299_1-1495145548`
  - Default (plugin is disabled): `kerberos_plugin_dir=NULL`
- 

## Linux-UNIX: Configuring the Kerberos plugin

To monitor database traffic on a server that uses Kerberos authentication, including identifying the DB\_USER, you must configure the `guardtap.ini` and `guardkerbplugin.conf` files appropriately.

## About this task

---

All customization settings for the Kerberos plugin are located in the file `guardkerbplugin.conf`. The default contents of this file are:

```
Kerberos values
KRB5RCACHETYPE=none
KRB5_KTNAME=/path/to/kerberos/krb5.keytab
KRB5_CONFIG=/path/to/kerberos/krb5.conf
Plugin values
KRB5_PLUGIN_CCACHE=/path/to/kerberos/krb5cc_*
KRB5_PLUGIN_GSSAPI_LIBRARY=/path/to/lib/libgssapi_krb5.so
#KRB5_PLUGIN_DEBUG=0
```

Lines beginning with a #, as well as blank lines, are treated as comments and ignored. Invalid entries cause errors and prevent the Kerberos plugin from running.

When any configuration entry is changed, the S-TAP must be restarted for the updated values to take effect.

Configuration entries are:

**KRB5RCACHETYPE**  
KRB5RCACHETYPE=none  
**KRB5\_KTNAME**  
This is the path to the keytab file; this can either be a keytab file already in use by the system, or one generated by Kerberos utilities specifically for use by the plugin. In general this file will have the name `krb5.keytab`, for example:  
KRB5\_KTNAME=/home/oracle11/krb5/keytab KRB5\_KTNAME=/home/sybase15/kerberos/keytab  
**KRB5\_CONFIG**  
This is the path to the Kerberos configuration file in use by the system. In general this file is named `krb5.conf`, for example:  
KRB5\_CONFIG=/home/oracle11/krb5/krb5.conf KRB5\_CONFIG=/home/sybase15/kerberos/krb5.conf  
**KRB5\_PLUGIN\_CCACHE**  
This is a wildcard path to where the Kerberos system cache files are located. For example:  
KRB5\_PLUGIN\_CCACHE=/tmp/krb5cc\*  
The value can also be a name if it is on the standard lib path, for example:  
KRB5\_PLUGIN\_CCACHE=<library name>.so  
Multiple paths can be specified, separated by a colon (:), for example:  
KRB5\_PLUGIN\_CCACHE=/home/sybase16/krb5cc\*: /tmp/krb5cc\*  
Note: Specifying more files than needed (for instance, specifying `/tmp/*`) impacts performance.  
**KRB5\_PLUGIN\_GSSAPI\_LIBRARY**  
This is the location of the Kerberos GSSAPI dynamic library. On most systems this is named `libgssapi_krb5.so`.  
The location can be specified by a full path, for example:  
KRB5\_PLUGIN\_GSSAPI\_LIBRARY=/usr/lib64/libgssapi\_krb5.so KRB5\_PLUGIN\_GSSAPI\_LIBRARY=/opt/freeware/lib64/libgssapi\_krb5.so  
Alternately, if the library is located on the standard library search path for the system, you can specify only the file name, for example:

KRB5\_PLUGIN\_GSSAPI\_LIBRARY=libgssapi\_krb5.so  
 Note: Any libraries that are needed by the GSSAPI library (typically libkrb5.so, libk5crypto.so, libkrbsupport.so) must also be on the system.  
 Important: If the Kerberos libraries are NOT in the standard library paths, you need to use the parameter KRB5\_PLUGIN\_GSSAPI\_LIBRARY. Uncomment it and update its value with full path of libgssapi\_krb5.so.

KRB5\_PLUGIN\_DEBUG  
 This parameter is used for debugging the plugin only. For normal operation this line must be commented out, or plugin performance is impacted.

## Procedure

---

1. In the guard\_tap.ini file, change the value of kerberos\_plugin\_dir parameter to the full path to the Guardium S-TAP, since that is where the plugin is located.
    - GIM installation: kerberos\_plugin\_dir=<guardium\_base>/modules/STAP/current
    - S-TAP shell installation: kerberos\_plugin\_dir=<guardium\_base>/guard\_stap
  2. Configure these in the guardkerbplugin.conf file that is also located in S-TAP installation directory:
    - KRB5\_KTNAME=<full path to kerberos krb5.keytab file>
    - KRB5\_CONFIG=<full path to kerberos krb5.conf file>
    - Optional parameters as described above. This configuration parameter for ticket cache might be required if the Kerberos plugin does not recognize the user. This parameter accepts wild cards as there is usually more than one cache file. You can specify multiple paths, separated by colons.
    - KRB5\_PLUGIN\_CCACHE=<full path to kerberos krb5cc\_\* files:additional full path to kerberos krb5cc\_\* files:etc>
- Note: In Guardium releases previous to V. 10.1.2, the parameters allow\_weak\_crypto = 1 and clockskew = 600 were required. In most cases these parameters are no longer required

## Linux-UNIX: Finding the Kerberos configuration parameters for Oracle

---

For Oracle Kerberos, locate the Kerberos keytab and configuration file locations in sqlnet.ora.

### About this task

---

## Procedure

---

1. Enter: **grep -i KERBEROS \$ORACLE\_HOME/network/admin/sqlnet.ora**  
 Output is similar to:  

```
SQLNET.AUTHENTICATION_KERBEROS5_SERVICE = oracle
SQLNET.KERBEROS5_CONF = /home/oracle11/krb5/krb5.conf
SQLNET.KERBEROS5_REALMS = /home/oracle11/krb5/krb.realms
SQLNET.AUTHENTICATION_SERVICES= (BEQ,KERBEROS5)
SQLNET.KERBEROS5_CLOCKSKW = 600
SQLNET.KERBEROS5_KEYTAB = /home/oracle11/krb5/keytab
SQLNET.KERBEROS5_CONF_MIT = TRUE
```
2. To find the Kerberos cache parameter, enter: **oklist|grep -i cache**  
 Output is similar to:  

```
Ticket cache: /tmp/krb5cc_500
```

## Linux-UNIX: Finding the Kerberos configuration parameters for Sybase

---

Use the Sybase environment variables to get the Kerberos information.

## Procedure

---

1. Enter: **klist -k**  
 Output is similar to:  

```
env|grep -i KRB
KRB5_KTNAME=/home/sybase15/kerberos/keytab
KRB5_CONFIG=/home/sybase15/kerberos/krb5.conf
```
2. To find the Kerberos cache parameter, enter: **klist -c**  
 Output is similar to:  

```
Ticket cache: FILE:/tmp/krb5cc_533
```

## Linux-UNIX: Merging keytab files

---

If you have multiple keytab files (for multiple databases on one host), you can merge the keys. After combining the keytabs, configure the Kerberos plugin to point to the one new combined keytab. Each database continues to use its own individual keytab, not the combined one.

## Procedure

---

1. Open the MIT Kerberos **ktutil** on your database server.
2. Write the 3 keytabs (filename 1, 2, 3) into the Kerberos V5 keytab file keytab, by entering, for example:

```

> ktutil
ktutil: read_kt <filename 1>
ktutil: read_kt <filename 2>
ktutil: read_kt <filename 3>
ktutil: write_kt krb5.keytab
ktutil: quit

```

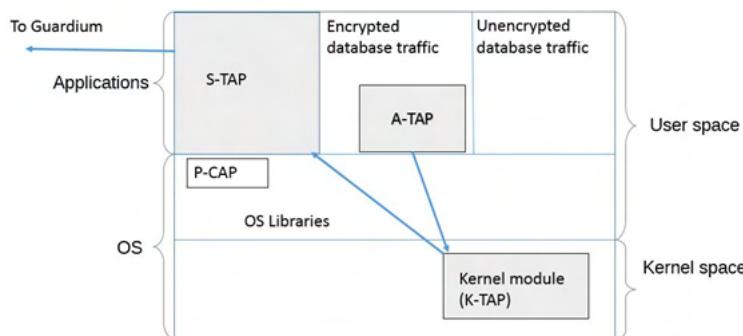
- Configure the Kerberos plugin to point to the one new combined keytab, in this example, **keytab**.

## Linux-UNIX: A-TAP management

A-TAP is an application-level tap. It sits in the application layer to support monitoring of encrypted database traffic, which cannot be done in the kernel by K-TAP.

The A-TAP mechanism monitors communication between internal components of the database server. The data is unencrypted in the application layer, where A-TAP picks it up and sends to K-TAP. K-TAP is a proxy to pass data to S-TAP, and from there it is then sent to the Guardium collector.

This figure shows where A-TAP fits in with the overall architecture on the database server.



A-TAP is included in every S-TAP but must be specifically configured for each database that requires it.

### When to use A-TAP

A-TAP is required when DBMS encryption in motion is used, but there may be other internal database implementation details such as shared memory that require it.

If you have the option, use an exit library instead of A-TAP.

### Limitations:

- A-TAP is not supported in an environment where a 32-bit database is located on a 64-bit server
- For ASO traffic, CLIENT\_IP is not the actual client IP; use the Analyzed Client IP, which is the correct IP.
- For Oracle ASO encrypted IPv6 traffic (local as well as remote), use the Client Host Name to identify the actual client session, due to limitations.
- For SSL traffic, CLIENT\_IP is not the actual client IP and there is no ANALYZED\_CLIENT\_IP.
- If CLIENT\_HOST\_NAME cannot be mapped to one specific network, it cannot be used to differentiate between multiple networks. In this case, ANALYZED\_CLIENT\_IP will not be available. Due to this limitation, use CLIENT\_HOST\_NAME to identify the actual client session.

Attention: The Exit interfaces for Db2® and Informix® are preferred to using A-TAP for Db2 and Informix. The Exit interfaces offer several advantages:

- No need to install or use kernel modules (K-TAP).
- Lower CPU utilization.
- New database versions are supported sooner.

A-TAP for Db2 and Informix are no longer supported starting with Guardium 12.0.

For information about using Db2 Exit, see [Linux-UNIX: Configuring Db2 Exit](#).

For information about using Informix Exit, see [Linux-UNIX: Configuring Informix Exit](#).

**Monitoring restrictions:** See [Guardium support matrix](#) for complete details on what is supported for the various databases and operating systems.

- [Linux-UNIX: Preparing for A-TAP configuration and maintenance](#)  
Configuring and maintaining A-TAP requires coordination with both the database and system administrators.
- [Linux-UNIX: A-TAP configuration and activation](#)  
Configure and activate each A-TAP.
- [Linux-UNIX: A-TAP activate, deactivate and DB stop, restart guidelines](#)  
Understand when to activate and deactivate A-TAP, and stop or restart the DB.
- [Linux-UNIX: guardctl utility commands for A-TAP](#)  
The guardctl utility is the A-TAP management tool. Understand these commands before starting to work with A-TAPS.
- [Linux-UNIX: guardctl return codes](#)  
The guardctl error codes clarify error conditions that occur, in particular, when you are call the guardctl script to manage ATAP instances via another script.
- [Linux-UNIX: Database-specific guardctl parameters](#)  
Each database type has specific guardctl requirements.
- [Linux-UNIX: Deactivating A-TAP](#)  
You must deactivate A-TAP before upgrading the database OS. You also need to deactivate the ATAPs before upgrading or uninstalling STAP (whether or not it's installed via GIM, RPM, or shell installer).
- [Linux-UNIX: Configuring and Activating A-TAP in Special Environments](#)  
Zones, WPARs, Teradata, and Oracle require additional configuration.
- [Linux-UNIX: Troubleshooting A-TAP configuration issues](#)  
This section summarizes common mistakes made during A-TAP configurations, their symptoms, and how to avoid them.

# Linux-UNIX: Preparing for A-TAP configuration and maintenance

Configuring and maintaining A-TAP requires coordination with both the database and system administrators.

To configure and activate A-TAP, the following authorities are needed:

- Either root access on the database server, or the database user.
- Authority to stop and restart the database

In addition, you must work with the DBA to get the required parameters to input into the utility. Details of the needed parameters are in [Linux-UNIX: Database-specific guardctl parameters](#). For ongoing maintenance, your organization must have documented procedures in place to handle the activation and deactivation of A-TAP during OS and database upgrades. See [Linux-UNIX: A-TAP activate, deactivate and DB stop, restart guidelines](#). For clustered environments, you need to configure and activate A-TAP on all nodes.

In most cases, use the Guardium guardctl utility to activate, upgrade, or deactivate A-TAP. See [Linux-UNIX: guardctl utility commands for A-TAP](#) for details on the syntax and options of the guardctl utility.

Before you begin:

- Make sure that the S-TAP is installed and K-TAP is enabled.
- Ensure that you have the root privileges on the database server.
- Consult [Linux-UNIX: Database-specific guardctl parameters](#) for your database to ensure you have the parameters you need to run the utility.

## Linux-UNIX: A-TAP configuration and activation

Configure and activate each A-TAP.

### About this task

Prerequisite:

- S-TAP and K-TAP are installed.
- If the software is installed with GIM, verify that GIM\_ROOT\_DIR is the absolute path to the modules, for example /usr/local/guardium/modules.
- The user must be authorized for the guardium group. If the guardium group was created in LDAP, then create a local group called guardium with the same group ID (when authorizing the DB user it is added to this group), OR add the guardium group ID (GID) to the DB user in /etc/passwd. For a shell installation, if the inspection engine db\_user is specified, then you don't need to authorize the user even in an LDAP environment.

There are two methods of managing your A-TAPs: either as user root for all functions, or as a db user. The db user option can configure, activate, deactivate, and instrument A-TAP, but cannot perform all functions. This means that the non-root user can handle day to day activities of the A-TAP, without requiring the root user. The guardctl help window lists the permitted commands for the logged-in user. The functionality is:

- When activating an A-TAP instance not as root, the current user must be the db\_user specified in the instance configuration, and must be specified as the db\_user for the matching inspection engine in the S-TAP configuration.
- A non-root user cannot manage (configure, active, deactivate, and instrument) an A-TAP instance that was initially configured by the root user.
- The root user can activate and deactivate a non-root created A-TAP instance, but must specify the instance name as \${DB\_USER}/\${DB\_INSTANCE}

Authorizing the user is optional. If you have db\_user specified in the guard\_tap.ini, you don't need to authorize the user, but you still may. If db\_user is not specified in the guard\_tap.ini, you must authorize the user and cannot perform any actions as non-root with guardctl.

### Procedure

1. Verify ktp\_installed=1 in the guard\_tap.ini file.
2. Log off from all active database sessions and stop the database. It is very important that all processes with database admin user are stopped. For example, on oracle, issue **ps -ef | grep oracle**

3. As root user, authorize the database administrative user to log traffic using the guardctl utility with the authorize-user command:  
`<guardium_base>/xxx/guardctl authorize-user <user-name>`

```
shell installer with postgres authorize user
/usr/local/guardium/guard_stap/guardctl authorize-user postgres Authorizing user 'postgres' to log traffic
shell installer with postgres verify authorization
/usr/local/guardium/guard_stap/guardctl is_user_authorized postgres User 'postgres' is authorized.
GIM installation with postgres authorize user
/usr/local/guardium/modules/ATAP/current/files/bin/guardctl authorize_user postgres Authorizing user 'postgres' to log traffic
shell installer example with Greenplum authorize user
/usr/local/guardium/guard_stap/guardctl authorize-user <gpadmin> Authorizing user '<gpadmin>' to log traffic
```

Note: If you're using MongoDB, restart the **mongod-mms-auto** process.

4. Store the configuration parameters:

- a. See [Linux-UNIX: Database-specific guardctl parameters](#) to determine the parameters needed for your database type and platform.
- b. Store configuration for the database instance using the store-conf command of the guardctl utility as follows.

```
<guardium_base>/xxx/guardctl db_instance=<instance> [<name>=<value> ...] store-conf
```

For example:

```
shell installer Oracle on Linux store-conf
/usr/local/guardium/guard_stap/guardctl --db-user=oracle11 --db-type=oracle --db-instance=on12rh60 --db-home=/home/oracle11/product/11.1.0/db_1 --db-version=11.2 store-conf
GIM installation Oracle on Linux store-conf
```

```

/usr/local/guardium/modules/ATAP/current/files/bin/guardctl db_instance=$ORACLE_SID db_home=$ORACLE_HOME db_type=oracle
db_user=oracle12 db_version=12 store-conf
shell installer Greenplum on Linux store-conf
/usr/local/guardium/guard_stap/guardctl --db-user=<gpadmin> --db-type=greenplum -db-home=<db_user home directory> --db-
instance=<greenplum> --db-base=<db_user home directory> store-conf

```

Note: Instrumentation is done automatically during activate; there is no explicit instrumentation.

#### 5. Activate A-TAP.

a. Enter <guardium\_base>/xxx/guardctl db\_instance=<instance> activate

```

shell installer Oracle on Linux activate
/usr/local/guardium/guard_stap/guardctl --db-instance=onrh60x activate
GIM installation Oracle on Linux activate
/usr/local/guardium/modules/ATAP/current/files/bin/guardctl --db-instance=onrh60x activate
shell installer Greenplum on Linux activate
/opt/guardium/guard_stap/guardctl --db-type=greenplum --db-home=/usr/local/greenplum-db-4.3.4.0 --db-user=gpadmin
--db-instance=greenplum --db-base=<db_user home directory> activate

```

You can activate and deactivate A-TAP by using the Encryption checkbox of the inspection engine configuration in the Guardium GUI, though there are no advantages to activating it in the GUI. This option is not available for Linux platforms.

b. Confirm that the instances are activated using the list-active command of the guardctl utility: <guardium\_base>/xxx/guardctl list-active

Example: <guardium\_base>/xxx/guardctl list-active oracle

#### 6. Start the database server.

#### 7. For SAP IQ (Sybase) 16.1 SP04 and higher, take the following steps to enable retrieval of the database user before you activate the A-TAP.

a. Create a stored procedure that calls the function 'guard' in the SybaseIQ ATAP library:

```
(DBA)> create or replace procedure CGuard (in p1 long varchar, in p2 long varchar) external name
'guard@/usr/lib64/libguard-atap-sybaseiq-any-64.so'
```

If the GNU C library (glibc) is lower than version 2.34, test that the call succeeds by executing the following command and verifying that it doesn't report an error. You can ignore the error messages if glibc is equal to or greater than version 2.34.

```
(DBA)> call CGuard(connection_property('UserID'),connection_property('Number'))
```

b. Create a login procedure:

```
(DBA)> create or replace procedure dba.login_msg_user() begin call dbo.sp_login_environment; call
CGuard(connection_property('UserID'),connection_property('Number')); end
```

c. Grant execute permissions to PUBLIC for the login procedure:

```
(DBA)> grant execute on DBA.login_msg_user to PUBLIC
```

d. Set the login procedure to execute for PUBLIC:

```
(DBA)> set option PUBLIC.login_procedure='DBA.login_msg_user'
```

Tip: After you activate the A-TAP, use the `ps -ef | grep dataserver` command to report on the running Sybase process (rather than `showserver`).

## Linux-UNIX: A-TAP activate, deactivate and DB stop, restart guidelines

Understand when to activate and deactivate A-TAP, and stop or restart the DB.

Restart/load/activated requirements for A-TAP.

| Scenario                                                       | Instructions                                                                    |
|----------------------------------------------------------------|---------------------------------------------------------------------------------|
| After installation of UNIX A-TAP in Oracle cluster environment | All database instances as well as all inter-cluster processes must be restarted |
| Before activating A-TAP                                        | Stop database                                                                   |
| After activating A-TAP                                         | Restart database                                                                |
| Before deactivating A-TAP                                      | Stop database                                                                   |
| Before upgrading database (for example applying Fixpack)       | Deactivate A-TAP                                                                |
| Before upgrading S-TAP                                         | Deactivate A-TAP                                                                |
| Before uninstalling S-TAP                                      | Deactivate A-TAP                                                                |

## Linux-UNIX: guardctl utility commands for A-TAP

The guardctl utility is the A-TAP management tool. Understand these commands before starting to work with A-TAPs.

### guardctl utility

There are two methods of managing your A-TAPs: either as user root for all functions, or as a db user. The db user option can configure, activate, deactivate, and instrument A-TAP, but cannot perform all functions. This means that the non-root user can handle day to day activities of the A-TAP, without requiring the root user. The guardctl help window lists the permitted commands for the logged-in user. The functionality is:

- When activating an A-TAP instance not as root, the current user must be the db\_user specified in the instance configuration, and must be specified as the db\_user for the matching inspection engine in the S-TAP configuration.
- A non-root user cannot manage (configure, active, deactivate, and instrument) an A-TAP instance that was initially configured by the root user.

- The root user can activate and deactivate a non-root created A-TAP instance, but must specify the instance name as \${DB\_USER}/\${DB\_INSTANCE}

Authorizing the user is optional. If you have db\_user specified in the guard\_tap.ini, you don't need to authorize the user, but you still may. If db\_user is not specified in the guard\_tap.ini, you must authorize the user and cannot perform any actions as non-root with guardctl.

The guardctl utility is installed under <guardium\_base>/guard\_stap directory where <guardium\_base> is the directory where Guardium® software is installed. In the case of a GIM installation guardctl it is installed under <guardium\_base>/modules/ATAP/current/files/bin.

#### Syntax

```
<guardium_base>/xxx/guardctl [<parameter>=<value>] [<parameter>=<value> ...] <command> [-q | -v | -qv]
```

See parameters in [Linux-UNIX: Database-specific guardctl parameters](#).

Note: Hyphen and underscore are interchangeable in the guardctl parameters.

## -q, -v, -qv flags

Use these flags to manage the output:

- q (quiet): suppress all output except name/value pairs
- v (value pairs): add name/value pairs related to each command
- qv: outputs name/value pairs only

The output depends on the type of command.

- Commands that take action across all configured instances
  - Print all name/value pairs for each instance except overall\_rv and overall\_msg
  - Print overall\_rv name/value pair at end where value is
    - 0 (success) if and only if all report success
    - 1 (failure) if any report any failure
  - Print overall\_msg name/value pair at end
  - Returns the value reported in the "overall\_rv" name/value pair
- Commands that take action on a single instance
  - Print all name/value pairs except overall\_rv and overall\_msg
  - Returns the value reported in the "rv" name/value pair
- Commands that store parameters, print parameters, or check status
  - Does not print name/value pairs

Name/Value pairs output looks like:

```
db_instance: ${db_instance}
db_user: ${db_user}
db_base: ${db_base}
db_home: ${db_base}
db_version: ${db_version}
db_type: ${db_type}
is_active: ${is_active} ("yes" or "no")
is_instrumented: ${is_db_instrumented} ("yes" or "no")
msg: some string
rv: ${retval}
overall_rv: ${retval}
overall_msg: (string)
```

## commands

| Command        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| activate       | Activates A-TAP for the specified database instance using the stored parameters. Outputs Name/Value pairs if -v or -qv specified. Activating an instance that's already active (whether DB is running or not) does not generate an error.                                                                                                                                                                                                                                     |
| authorize-user | Adds the user to 'guardium' authorization group.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| db_console_log | Enables the A-TAP console log. Valid values: <ul style="list-style-type: none"> <li>0: disable, log only error level info</li> <li>1: enable</li> </ul> Default = 0                                                                                                                                                                                                                                                                                                           |
| deactivate     | Deactivates the A-TAP for the specified, single database instance. Outputs Name/Value pairs if -v or -qv specified. Deactivating an instance that's already inactive (whether DB is running or not) does not generate an error.                                                                                                                                                                                                                                               |
| deactivate-all | Deactivates A-TAP for a specified list of database instances. If no database instances are specified, all active A-TAPs are deactivated. Outputs Name/Value pairs for each instance, if -v or -qv specified. You can optionally specify the db-type to deactivate a group (e.g. all Oracle). For additional name/value pair, specify "overall_rv={0,1}" at end. Returns success (0) if rv=0 for every instance. Returns failure (1) if at least one instance reports rv != 0. |
| deinstrument   | Removes instrumentation for the specified Oracle DB. Not required from v10.1 and higher. If deinstrumentation is required, it is done automatically during deactivate. Outputs Name/Value pairs if -v or -qv specified. Deinstrumenting an instance that is not instrumented does not generate an error, even if the is DB running, regardless of activation status.                                                                                                          |
| dump-params    | Dumps current values of parameters                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| get-statistics | Get A-TAP statistics. Statistics includes information about which ATAPs are active, which are inactive, and which are in an incorrect in-between state (this shouldn't happen, it usually occurs when someone updates the DB while ATAP is active).                                                                                                                                                                                                                           |
| help           | Default command, prints the list of supported commands, parameters and their default values. Use this to see which commands you can execute, depending on your user type.                                                                                                                                                                                                                                                                                                     |
| instrument     | Explicitly creates relinked instrumented Oracle. If instrumentation is required, it is usually done automatically during activate. Manual instrumentation is only required for Oracle versions <= 10 on AIX. Instrumenting an already instrumented instance returns an error. Outputs Name/Value pairs if -v or -qv specified.                                                                                                                                                |

| Command              | Description                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| is-active            | Returns 1 if there is at least one A-TAP activated instance. Otherwise, returns 0.                                                                                                                                                                                                                                                                                                 |
| is-user-authorized   | Checks whether the db-user (running A-TAP) is authorized to the guardium group, and can log database traffic to K-TAP/S-TAP.                                                                                                                                                                                                                                                       |
| list-active          | Lists database instance user names of all active A-TAP database instances. Outputs Name/Value pairs if -v or -qv specified.                                                                                                                                                                                                                                                        |
| list-configured      | Lists database instances with configured but inactive A-TAPs. Outputs Name/Value pairs if -v or -qv specified.                                                                                                                                                                                                                                                                     |
| oracle-relink        | Calls the utility provided by oracle to relink the DB binary.                                                                                                                                                                                                                                                                                                                      |
| prepare-libs         | Prepares libraries for use in Zone/WPAR installation                                                                                                                                                                                                                                                                                                                               |
| repair               | Run this command if the DB is (accidentally) upgraded while the A-TAP is active. It renames the -guard-original and -guard-instrumented files. Returns success on successful repair or if repair is not necessary. Does not touch the current DB executable. Outputs Name/Value pairs if -v or -qv specified. From v10.1.4, it is called automatically on activate and deactivate. |
| restore-active-ataps | Restores the active state of the A-TAPs previously saved via save-active-ataps. If an instance fails to activate (due to DB running or some other error), then the remaining instances still attempt to activate. This command can be run multiple times without problem, since activating an already active instance is not an error.                                             |
| save-active-ataps    | Saves the configurations for the currently active A-TAPs in a single file so that they can be restored later to an active state. Useful prior to deactivate-all when preparing to upgrade DBs.                                                                                                                                                                                     |
| store-conf           | Stores the configuration for a particular database instance                                                                                                                                                                                                                                                                                                                        |
| store-system-conf    | Stores the system configuration parameters                                                                                                                                                                                                                                                                                                                                         |

## Linux-UNIX: guardctl return codes

The guardctl error codes clarify error conditions that occur, in particular, when you are call the guardctl script to manage ATAP instances via another script.

| Code | Description                                                                                                   | Usage                                                                                                                                                                                                                                                              |
|------|---------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0    | success                                                                                                       | Returned by every command.<br>When returned in response to deactivate, all instances are deactivated<br>When returned in response to is-active, there are no active instances                                                                                      |
| 1    | bad parameter                                                                                                 | Returned by every command when a parameter is invalid or missing                                                                                                                                                                                                   |
| 2    | is-active called on unrecognized instance                                                                     | Returned by is-active when a db-instance specified is not known to guardctl and as such cannot be determined to be active or not                                                                                                                                   |
| 20   | attempted to activate instance while database was running, but not yet active                                 | Returned by activate to indicate that the DB instance is running, so activation could not take place                                                                                                                                                               |
| 21   | attempted to deactivate instance while database was running, but not yet inactive                             | Returned by deactivate to indicate that the DB instance is running, so deactivation could not take place                                                                                                                                                           |
| 22   | user is not authorized                                                                                        | Returned by instrument and activate to indicate that the db-user specified is not authorized as a member of the 'guardium' group. Run authorize-user to correct.                                                                                                   |
| 23   | db-home parameter doesn't match db_install_dir parameter in guard_tap.ini                                     | Returned by store-conf and activate to indicate that the current guard_tap.ini doesn't have an IE configured with a db_home that matches the db_install_dir ATAP parameter. One of those needs to be adjusted to the correct value or STAP may not run.            |
| 24   | attempt to deactivate an instance where the executable is neither an ATAP executor or the instrumented binary | Returned by deactivate. This instance looks like it should be activated, but the binary isn't what it should be if it is. DB executable could have been updated while ATAP was active. Run the repair command to fix the issue and activate again.                 |
| 25   | attempt to activate atap when encryption=1 set in guard_tap.ini                                               | Returned by activate when the encryption parameter is set to 1 in the IE. Do not activate with guardctl and use the encryption parameter in the ini.                                                                                                               |
| 26   | db executable file not found                                                                                  | Returned by activate, deactivate, instrument, deinstrument, store-conf, prepare-libs, and repair. The DB executable is missing (e.g. the oracle binary itself is not in the path specified). Check the path parameters used when configuring the instance.         |
| 27   | instrumentation required but not done                                                                         | Returned by activate and store-conf when instrumentation is required, but has not already been done. Oracle instrumentation is now automatically done in most cases, but still needs to be manually specified for AIX and Oracle versions <= 10.                   |
| 28   | is-active reports instance is not active                                                                      | Returned by is-active. Informational only. The db-instance specified is not active or if no instances were specified, no instances are active.                                                                                                                     |
| 29   | deactivate-all not complete success                                                                           | Returned by deactivate-all when at least one active instance could not be deactivated.                                                                                                                                                                             |
| 30   | is-instrumented reports instance is not instrumented                                                          | Not exported via command.                                                                                                                                                                                                                                          |
| 40   | internal instrumentation error                                                                                | Returned by instrument when instrumentation couldn't be completed.                                                                                                                                                                                                 |
| 41   | internal instrumentation error                                                                                | Returned by instrument when instrumentation couldn't be completed.                                                                                                                                                                                                 |
| 42   | internal instrumentation error                                                                                | Returned by instrument when instrumentation couldn't be completed.                                                                                                                                                                                                 |
| 43   | instrumentation error, cannot save original binary                                                            | Returned by instrument when the -guard-original file already exists. Either A-TAP is currently active with instrumentation, or A-TAP is inactive but the instrumentation is still active. Deactivate and deinstrument before subsequent instrument and activate.   |
| 44   | attempt to instrument while instance running and not already instrumented                                     | Returned by instrument when DB instance is currently running. Stop DB instance before attempting to instrument again.                                                                                                                                              |
| 45   | attempt to instrument while A-TAP is active and not already instrumented                                      | Returned by instrument when A-TAP is already active, but instrumentation is not active. This can happen when switching from an Oracle configuration that doesn't require instrumentation to one that does. Deactivate A-TAP before attempting to instrument again. |
| 46   | attempt to instrument and already instrumented instance                                                       | Returned by instrument while instance is already instrumented. If instrumentation needs to be redone, deinstrument first.                                                                                                                                          |

| Code | Description                                                                                                                | Usage                                                                                                                                                                                                                                                                    |
|------|----------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 93   | unspecified error due to DB running not when activating, deactivating, or instrumenting (e.g. when running repair command) |                                                                                                                                                                                                                                                                          |
| 94   | no atap library supporting this db                                                                                         | Returned by instrument, deinstrument, prepare-libs, activate, deactivate, repair, list-active, and list-configured. Usually indicates that an unknown error occurred.                                                                                                    |
| 95   | system error, cannot find group                                                                                            | Returned by activate. The guardium group doesn't appear to be known to this system.                                                                                                                                                                                      |
| 96   | system error, cannot create group                                                                                          | Returned by authorize-user. The guardium group did not exist and an attempt to create the group failed.                                                                                                                                                                  |
| 97   | filesystem error, cannot create directory or file, or insufficient space detected                                          |                                                                                                                                                                                                                                                                          |
| 98   | platform unsupported                                                                                                       | Returned by instrument, deinstrument, prepare-libs, activate, deactivate, repair, list-active, list-configured, store-conf. The DB you're trying to use with ATAP is not supported on this platform (e.g. DB2, Informix, teradata, or mongo on anything but Linux, etc). |
| 99   | other unspecified error                                                                                                    |                                                                                                                                                                                                                                                                          |

## Linux-UNIX: Database-specific guardctl parameters

Each database type has specific guardctl requirements.

- [Linux-UNIX: Db2-specific guardctl parameters](#)  
Use these guardctl parameters when configuring A-TAP for a Db2 database, Linux only.
- [Linux-UNIX: Informix-specific guardctl parameters](#)  
Use these guardctl parameters when configuring A-TAP for a Informix database.
- [Linux-UNIX: Greenplum-specific guardctl parameters](#)  
Use these guardctl parameters when configuring A-TAP for a Greenplum database.
- [Linux-UNIX: Mongo-specific guardctl parameters](#)  
Use these guardctl parameters when configuring A-TAP for a MongoDB database.
- [Linux-UNIX: Oracle-specific guardctl parameters](#)  
Use these guardctl parameters when configuring A-TAP for an Oracle database.
- [Linux-UNIX: Postgres-specific guardctl parameters](#)  
Use these guardctl parameters when configuring A-TAP for a Postgres database.
- [Linux-UNIX: Sybase-specific guardctl parameters](#)  
Use these guardctl parameters when configuring A-TAP for a Sybase database.
- [Linux-UNIX: Sybase IQ-specific guardctl parameters](#)  
Use these guardctl parameters when configuring A-TAP for a Sybase database.
- [Linux-UNIX: Teradata-specific guardctl parameters](#)  
Use these guardctl parameters when configuring A-TAP for a Teradata database.
- [Linux-UNIX: Vertica-specific guardctl parameters](#)  
Use these guardctl parameters when configuring A-TAP for a Vertica database.

## Linux-UNIX: Db2-specific guardctl parameters

Use these guardctl parameters when configuring A-TAP for a Db2 database, Linux only.

### Db2 (Linux only) required parameters

**Example:**

```
/usr/local/guardium/guard_stap/guardctl --db-user=db2inst1 --db-type=db2 --db-instance=dn0rh7x6 --db-version=10.5 store-conf
```

The script **find\_db2\_shmem\_parameters.sh**, located in `stap_directory/bin`, outputs what the Db2 shared memory parameters defined in the Inspection Engines should be. Execute it either as root or Db2 user, using the syntax: **find\_db2\_shmem\_parameters.sh <instance name>**. You can run it from any directory.

Note: Hyphen and underscore are interchangeable in the guardctl parameters.

| Required Parameter | Value                | How to determine                    |
|--------------------|----------------------|-------------------------------------|
| db_user            | Db2 username         | Points to the DB instance user name |
| db_instance        | Db2 instance name    | \$ db2 LIST DATABASE DIRECTORY      |
| db_type            | db2                  |                                     |
| db_version         | The database version | As Db2 user: \$ db2level            |

### Db2 (Linux only) optional parameters

| Optional Parameter | Value                                  | How to determine                                                                                      | When is it required                                               |
|--------------------|----------------------------------------|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| db_home            | Path where the DB version is installed | Same as db_base                                                                                       |                                                                   |
| db_base            | Database instance user home directory  | Value for db_base must match the correct path DB instance user home directory. It cannot be ~DB_USER. | Where db_base is not same as db_home                              |
| db_bits            | 32 or 64                               | DB instance architecture (32 for 32-bit, 64 for 64-bit)                                               | Required only if A-TAP is not able to recognize the architecture. |

| Optional Parameter | Value  | How to determine                     | When is it required                          |
|--------------------|--------|--------------------------------------|----------------------------------------------|
| db2_shmsize        | 131072 | Db2 shared memory size               | When the value is different than the default |
| db2_c2soffset      | 61440  | Db2 shared memory client area offset | When the value is different than the default |
| db2_header_offset  | 20     | Db2 shared memory header offset      | When the value is different than the default |

## Linux-UNIX: Informix-specific guardctl parameters

Use these guardctl parameters when configuring A-TAP for a Informix database.

### Informix required parameters

**Example:**

```
/usr/local/guardium/guard_stap/guardctl --db-user=informix --db-type=informix --db-instance=in17rh7x --db-version=11.70 store-conf
```

Note: Hyphen and underscore are interchangeable in the guardctl parameters.

| Required Parameter | Value                  | How to determine                    |
|--------------------|------------------------|-------------------------------------|
| db_user            | Informix username      | Points to the DB instance user name |
| db_instance        | Informix instance name | Informix Server instance name       |
| db_type            | informix               |                                     |
| db_version         | The database version   | As Informix user: dbaccess -V       |

### Informix optional parameters

| Optional Parameter | Value                                       | How to determine                                                                                                                       | When is it required                  |
|--------------------|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| db_home            | Points to where the DB version is installed | Same as db_base                                                                                                                        |                                      |
| db_base            | Home directory of db_user                   | DB instance user home directory. Value for db_base must match the correct path DB instance user home directory. It cannot be ~DB_USER. | Where db-base is not same as db-home |
| db_bits            | 32 or 64                                    | DB instance architecture (32 for 32-bit, 64 for 64-bit)                                                                                |                                      |

## Linux-UNIX: Greenplum-specific guardctl parameters

Use these guardctl parameters when configuring A-TAP for a Greenplum database.

Important: When A-TAP is configured, blocking (S - GATE) and redaction are not supported.

### Greenplum required parameters

**Example:**

```
/opt/guardium/guard_stap/guardctl --db-type=greenplum --db-home=/usr/local/greenplum-db-4.3.4.0 --db-user=gpadmin --db-instance=greenplum --db-base=/usr/local/greenplum-db-4.3.4.0 activate
```

Note: Hyphen and underscore are interchangeable in the guardctl parameters.

| Required Parameter | Value                                 | How to determine                                                                                                                                                                                           |
|--------------------|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| db_base            | Database instance user home directory | Required when db_user is different than the OS user for the DB. In this case, the db_base value should be set also in the guard_tap.ini parameter db_install_dir, for the corresponding Inspection Engine. |
| db_home            | Path where the database is installed. |                                                                                                                                                                                                            |
| db_instance        | Greenplum instance name               | User-defined string that identifies this instance                                                                                                                                                          |
| db_type            | Greenplum                             |                                                                                                                                                                                                            |
| db_user            | Greenplum user name                   | OS user for the database .or user that owns the process for the database executable                                                                                                                        |

## Linux-UNIX: Mongo-specific guardctl parameters

Use these guardctl parameters when configuring A-TAP for a MongoDB database.

Important: When A-TAP is configured, blocking (S - GATE) and redaction are not supported.

### Mongo required parameters

**Example:**

```
/opt/guardium/guard_stap/guardctl --db-type=mongodb --db-instance=mongodb36 --db-user=mongodb36 --db-base=/home/mongodb36 --db-home=/home/mongodb36/mongodb-linux-x86_64-enterprise-rhel62-3.6.5 activate
```

Note: Hyphen and underscore are interchangeable in the guardctl parameters.

| Required Parameter | Value                                                                                                                         | How to determine                                                                                                                                                                                           |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| db_base            | Database instance user home directory                                                                                         | Required when db_user is different than the OS user for the DB. In this case, the db_base value should be set also in the guard_tap.ini parameter db_install_dir, for the corresponding Inspection Engine. |
| db_home            | Path where the database is installed.                                                                                         |                                                                                                                                                                                                            |
| db_instance        | MongoDB instance name                                                                                                         | User-defined string that identifies this instance                                                                                                                                                          |
| db_type            | <ul style="list-style-type: none"> <li>• Servers running mongod: mongodb</li> <li>• Servers running mongos: mongos</li> </ul> |                                                                                                                                                                                                            |
| db_user            | MongoDB user name                                                                                                             | OS user for the database .or user that owns the process for the database executable                                                                                                                        |

## Linux-UNIX: Oracle-specific guardctl parameters

Use these guardctl parameters when configuring A-TAP for an Oracle database.

**Example:**

```
/usr/local/guardium/guard_stap/guardctl --db-user=oracle11 --db-type=oracle --db-instance=on12rh60 --db-home=/home/oracle11/product/11.1.0/db_1 --db-base=/home/oracle11 --db-version=11.2 store-conf
```

Note: Hyphen and underscore are interchangeable in the guardctl parameters.

## Oracle required parameters

| Required Parameter | Value                                                                 | How to determine                                                                                                                       |
|--------------------|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| db_user            | Oracle user name                                                      | Use the database instance user name.                                                                                                   |
| db_instance        | Oracle instance name                                                  | Use the value from \$ORACLE_SID                                                                                                        |
| db_type            | Oracle                                                                |                                                                                                                                        |
| db_home            | DB HOME. for example \$ORACLE_HOME                                    | DB admin has these details.                                                                                                            |
| db_base            | Database instance user home directory (Database owner home directory) | DB owner \$HOME (~DB_USER), and must match db_install_dir in the corresponding Inspection Engine. See <a href="#">db_install_dir</a> . |
| db_version         | The database version                                                  | Run SQL > SELECT * FROM V\$VERSION                                                                                                     |

## Oracle optional parameters

| Optional Parameter  | Value    | How to determine                                                                                                   | When is it required                                                                                                                                                                                                                                                                                                                                     |
|---------------------|----------|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| db_relink           | No/yes   | A-TAP activation method                                                                                            |                                                                                                                                                                                                                                                                                                                                                         |
| db_use_instrumented | No/yes   | A-TAP activation uses a relinked version of Oracle previously created with the <b>guardctl instrument</b> command. | <p>Instrumentation is required for:</p> <ul style="list-style-type: none"> <li>• Oracle 12 and later SSL for all non-Windows platforms</li> <li>• Oracle SSL on AIX</li> <li>• Oracle ASO prior to Oracle 11.2 on AIX</li> </ul> <p>Instrumentation is automatic when Oracle is linked from the <b>activate</b> command or through the Guardium UI.</p> |
| db_bits             | 32 or 64 | DB instance architecture (32 for 32-bit, 64 for 64-bit)                                                            | Required only if A-TAP is not able to recognize the architecture.                                                                                                                                                                                                                                                                                       |

## Linux-UNIX: Postgres-specific guardctl parameters

Use these guardctl parameters when configuring A-TAP for a Postgres database.

## Postgres required parameters

**Example:**

```
/usr/local/guardium/guard_stap/guardctl --db-user=postgres --db-type=postgres --db-instance=guardium_qa --db-version=9.4 --db-base=/home/postgres94 store-conf
```

Note: Hyphen and underscore are interchangeable in the guardctl parameters.

| Required Parameter | Value             | How to determine                    |
|--------------------|-------------------|-------------------------------------|
| db-user            | Postgres username | Points to the DB instance user name |

| Required Parameter | Value                  | How to determine                      |
|--------------------|------------------------|---------------------------------------|
| db_instance        | Postgres instance name | Postgres Server instance name         |
| db_type            | postgres               |                                       |
| db_version         | The database version   | As Postgres user:<br>pg_ctl --version |

## Postgres optional parameters

| Optional Parameter | Value                                       | How to determine                                                                                                                       | When is it required                  |
|--------------------|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| db_home            | Points to where the DB version is installed | Same as db_base                                                                                                                        |                                      |
| db_base            | Home directory of db_user                   | DB instance user home directory. Value for db_base must match the correct path DB instance user home directory. It cannot be ~DB_USER. | Where db-base is not same as db-home |
| db_bits            | 32 or 64                                    | DB instance architecture (32 for 32-bit, 64 for 64-bit)                                                                                |                                      |
| db_tcp_min_port    | 0 to any integer                            | Low end of TCP port range to intercept                                                                                                 | Using Real IPs                       |
| db_tcp_max_port    | 0 to any integer                            | High end of TCP port range to intercept                                                                                                | Using Real IPs                       |

## Linux-UNIX: Sybase-specific guardctl parameters

Use these guardctl parameters when configuring A-TAP for a Sybase database.

## Sybase required parameters

### Example:

```
/usr/local/guardium/guard_stap/guardctl --db-user=sybase15 --db-type=sybase --db-instance=sn57rh7x --db-version=15 store-conf
```

Note: Hyphen and underscore are interchangeable in the guardctl parameters.

| Required Parameter | Value                                     | How to determine                                                                               |                                                                                                                                                                                                           |
|--------------------|-------------------------------------------|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| db_home            | Points to where the database is installed | Same as db_base                                                                                | The basis for how we look for the DB binary. It can usually use the value of db_base, though it's immediately apparent when activating if it's wrong (guardctl complains about not finding the DB binary) |
| db_instance        | Sybase instance name                      | Sybase Server instance name. This parameter is used to name the ATAP instance within guardctl. |                                                                                                                                                                                                           |
| db_tcp_max_port    | 0 to any integer                          | High end of TCP port range to intercept. Use real IPs.                                         |                                                                                                                                                                                                           |
| db_tcp_min_port    | 0 to any integer                          | Low end of TCP port range to intercept. Use real IPs.                                          |                                                                                                                                                                                                           |
| db_type            | sybase                                    |                                                                                                |                                                                                                                                                                                                           |
| db_user            | Sybase user name                          | The database instance user name. Use the value of the guard_tap.ini parameter: db_user         |                                                                                                                                                                                                           |
| db_version         | The database version                      | As Sybase user:<br>> select @@version<br>> go                                                  |                                                                                                                                                                                                           |

## Sybase optional parameters

| Optional parameter           | Value                                 | How to determine                                                                                                                                                  | When is it required                                                                                                                                                                                                                                                                                                                        |
|------------------------------|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| db_base                      | Database instance user home directory | DB instance user home directory. this needs to match db_install_dir in some IE in the guard_tap.ini. Do not use the ~DB_USER shortcut, use the full path instead. | If you aren't specifying db_home separately, use the value for db_base as the value for db_home.                                                                                                                                                                                                                                           |
| db_bits                      | 32 or 64                              | DB instance architecture (32 for 32-bit, 64 for 64-bit)                                                                                                           | Required only if A-TAP is not able to recognize the architecture.                                                                                                                                                                                                                                                                          |
| -db-tcp-intercepted-ports    | 0 to any integer                      | TCP ports to intercept                                                                                                                                            | Specifies whether you want the real IP reported for encrypted sessions. There are potential performance impacts in this mode, and an added complication to the A-TAP setup by specifying this port. Leave blank to use the non-specific IP mode. This parameter is mutually exclusive with db_tcp_min_port and db_tcp_max_port parameters. |
| db-tcp-max-associate-time-ms | 1 to any integer                      |                                                                                                                                                                   | Ensure this parameter has a value. Otherwise it might drop some database connections for concurrent sessions. Default = 2500                                                                                                                                                                                                               |

## Linux-UNIX: Sybase IQ-specific guardctl parameters

Use these guardctl parameters when configuring A-TAP for a Sybase database.

### Sybase IQ required parameters

#### Example:

```
/usr/local/guardium/guard_stap/guardctl --db-user=sybase --db-type= sybaseiq --db-instance= sybaseiq --db-version=16.1 store-conf
```

Note: Hyphen and underscore are interchangeable in the guardctl parameters.

| Required Parameter | Value                | How to determine                                                                                                                                                                             |
|--------------------|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| db_instance        | Sybase instance name | Sybase Server instance name (could be any name to identify the environment)                                                                                                                  |
| db_type            | sybaseiq             |                                                                                                                                                                                              |
| db_user            | Sybase user name     | The Sybase IQ account owner                                                                                                                                                                  |
| db_version         | The database version | As Sybase user:<br><br><pre>\$ start_iq -v<br/>SAP IQ/16.1.040.1175/12886/P/SP04.02/Linux/Linux64 - x86_64 - 3.10.0-327/64bit/2019-09-24<br/>17:40:48<br/>[sybiq16@rh7u5x64t-ktap ~]\$</pre> |
| db_tcp_max_port    | 0 to any integer     | High end of TCP port range to intercept. Use real IPs.                                                                                                                                       |
| db_tcp_min_port    | 0 to any integer     | Low end of TCP port range to intercept. Use real IPs.                                                                                                                                        |

### Sybase IQ optional parameters

| Optional Parameter           | Value                                     | How to determine                                                                                                                       | When is it required                                                                                                                                                                                                                                                                                                                        |
|------------------------------|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| db_home                      | Points to where the database is installed | <b>echo \$SYBASE</b> or <b>echo \$SYBROOT</b> from Sybase IQ user environment                                                          | Where db-home is not in the same path as DB user HOME directory                                                                                                                                                                                                                                                                            |
| db_base                      | Home directory of db_user                 | DB instance user home directory. Value for db_base must match the correct path DB instance user home directory. It cannot be ~DB_USER. | Should match value for db_install_dir for corresponding Inspection Engine in guard_tap.ini                                                                                                                                                                                                                                                 |
| db_bits                      | 32 or 64                                  | DB instance architecture (32 for 32-bit, 64 for 64-bit)                                                                                |                                                                                                                                                                                                                                                                                                                                            |
| -db-tcp-intercepted-ports    | 0 to any integer                          | TCP ports to intercept                                                                                                                 | Specifies whether you want the real IP reported for encrypted sessions. There are potential performance impacts in this mode, and an added complication to the A-TAP setup by specifying this port. Leave blank to use the non-specific IP mode. This parameter is mutually exclusive with db_tcp_min_port and db_tcp_max_port parameters. |
| db-tcp-max-associate-time-ms | 1 to any integer                          |                                                                                                                                        | Ensure this parameter has a value. Otherwise it might drop some database connections for concurrent sessions. Default = 2500                                                                                                                                                                                                               |

## Linux-UNIX: Teradata-specific guardctl parameters

Use these guardctl parameters when configuring A-TAP for a Teradata database.

### Examples of commands

Store A-TAP configuration:

```
/usr/local/guardium/guard_stap/guardctl --dbinstance=teradata --tdc_gtwgateway=/usr/tgtw/bin/gtwgateway --db-type=teradata --db-home=/opt/teradata/tdat/pde/15h.00.00.07 --dbuser=teradata store-conf
```

Activate A-TAP:

```
/usr/local/guardium/guard_stap/guardctl -db instance=teradata activate
```

Start Teradata instance:

```
/etc/init.d/tpa start
Teradata Database Initiator service is starting...
Teradata Database Initiator service started successfully.
/etc/init.d/tgtw start
tgtw Startup complete
```

### Teradata required parameters

Note: Hyphen and underscore are interchangeable in the guardctl parameters.

| Required Parameter | Value                                                                                                                                                         | How to determine                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| db_instance        | typically teradata                                                                                                                                            | Teradata Server instance name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| db_home            | Points to where the DB version is installed, one of: <ul style="list-style-type: none"><li>• /opt/teradata/tdat/pde/15h.00.00.07</li><li>• /usr/pde</li></ul> | Determine the path to pdomain. Typically, the path is: /usr/pde/bin/pdomain.<br><br><pre># ls -l /proc/4608/exe lrwxrwxrwx 1 root tdrtrusted 0 2015-01-03 01:20 /proc/4608/root 20620 20063 0 12:40 pts/0 00:00:00 grep pdomain/exe -&gt; /opt/teradata/tdat/pde/15h.00.00.07/bin/pdomain</pre> Check the inodes for this file and /usr/pde/bin/pdomain to find out if they are the same:<br><br><pre># ls -li /opt/teradata/tdat/pde/15h.00.00.07/bin/pdomain 1638875 -r-xr-xr-x 1 teradata tdrtrusted 1294666 2014-01-22 01:40 # ls -li /usr/pde/bin/pdomain 1638875 -r-xr-xr-x 1 teradata tdrtrusted 1294666 2014-01-22 01:40</pre> Since the inodes are the same and the default value for --dbhome=/usr/pde, the parameter in this case does not need to be set. Otherwise, it can be set one of: <ul style="list-style-type: none"><li>• --db-home=/opt/teradata/tdat/pde/15h.00.00.07</li><li>• --db-home=/usr/pde</li></ul> |
| db_type            | teradata                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| db_user            | teradata                                                                                                                                                      | Determine the user running gtwgateway and path, for example:<br><br><pre># ps -ef   grep gtwgateway teradata 5000 4608 0 Jan03 ? 00:00:05 /usr/tgtw/bin/gtwgateway</pre> gtwgateway runs as user teradata.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| tdc_gtwgateway     | /usr/tgtw/bin/gtwgateway                                                                                                                                      | Default path to gtwgateway is /usr/tgtw/bin/gtwgateway, otherwise the tdc_gtwgateway parameter should be configured: --tdc_gtwgateway=/usr/tgtw/bin/gtwgateway                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## Teradata optional parameters

| Optional Parameter | Value                     | How to determine                                                                                                                       | When is it required                  |
|--------------------|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| db_base            | Home directory of db_user | DB instance user home directory. Value for db_base must match the correct path DB instance user home directory. It cannot be ~DB_USER. | Where db_base is not same as db_home |
| db_bits            | 32 or 64                  | DB instance architecture (32 for 32-bit, 64 for 64-bit)                                                                                |                                      |

## Linux-UNIX: Vertica-specific guardctl parameters

Use these guardctl parameters when configuring A-TAP for a Vertica database.

## Vertica required parameters

### Example:

```
/usr/local/guardium/guard_stap/guardctl --db-user=vertica --db-type=vertica --db-instance=guardium_qa --db-version=9.4 --db-base=/home/vertica94 store-conf
```

Note: Hyphen and underscore are interchangeable in the guardctl parameters.

| Required Parameter | Value                 | How to determine                     |
|--------------------|-----------------------|--------------------------------------|
| db_user            | vertica username      | Points to the DB instance user name  |
| db_instance        | Vertica instance name | Vertica Server instance name         |
| db_type            | vertica               |                                      |
| db_version         | The database version  | As Vertica user:<br>pg_ctl --version |

## Vertica optional parameters

| Optional Parameter | Value                                       | How to determine                                                                                                                       | When is it required                  |
|--------------------|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| db_home            | Points to where the DB version is installed | Same as db_base                                                                                                                        |                                      |
| db_base            | Home directory of db_user                   | DB instance user home directory. Value for db_base must match the correct path DB instance user home directory. It cannot be ~DB_USER. | Where db-base is not same as db-home |
| db_bits            | 32 or 64                                    | DB instance architecture (32 for 32-bit, 64 for 64-bit)                                                                                |                                      |
| db_tcp_min_port    | 0 to any integer                            | Low end of TCP port range to intercept                                                                                                 | Using Real IPs                       |
| db_tcp_max_port    | 0 to any integer                            | High end of TCP port range to intercept                                                                                                | Using Real IPs                       |

## Linux-UNIX: Deactivating A-TAP

You must deactivate A-TAP before upgrading the database OS. You also need to deactivate the ATAPs before upgrading or uninstalling STAP (whether or not it's installed via GIM, RPM, or shell installer).

## About this task

---

### Procedure

---

1. Make sure the database is stopped. Log off from all active database sessions.
2. Deactivate A-TAP for the database:

```
general example
 <guardium_base>/xxx/guardctl -db-instance=<instance-name> deactivate
Greenplum example
 /opt/guardium/guard_stap/guardctl --db-instance=<instance-name> deactivate
```

3. Alternately, deactivate all active instances by running:  
`<guardium_base>/xxx/guardctl deactivate-all`

## Linux-UNIX: Configuring and Activating A-TAP in Special Environments

---

Zones, WPARs, Teradata, and Oracle require additional configuration.

- [Linux-UNIX: Activating A-TAP for Oracle on a Veritas Cluster](#)

S-TAP includes an A-TAP feature required for Oracle deployments which use encryption. This task describes activating A-TAP in this Oracle Veritas Clustering nodes.

- [Linux-UNIX: Installing and activating A-TAP in Solaris zones](#)

Installing A-TAP in Solaris zones requires additional configuration.

- [Linux-UNIX: Installing and activating A-TAP in WPARs environment](#)

Installing A-TAP in WPARs requires additional configuration.

- [Linux-UNIX: Deactivate and uninstall A-TAP in Zones and WPARs environment](#)

- [Linux-UNIX: Upgrading A-TAP in Zones and WPARs environment](#)

- [Linux-UNIX: Configure and activate A-TAP steps for Teradata database](#)

- [Linux-UNIX: Oracle considerations for A-TAP](#)

## Linux-UNIX: Activating A-TAP for Oracle on a Veritas Cluster

---

S-TAP includes an A-TAP feature required for Oracle deployments which use encryption. This task describes activating A-TAP in this Oracle Veritas Clustering nodes.

### About this task

---

This procedure uses typical file paths for a shell installation. The GIM procedure is the same, but with different paths. For example:  
`/opt/guardium/modules/ATAP/current/files/bin/guardctl`.

### Procedure

---

1. Set up A-TAP on all nodes without activation. For example:

```
/opt/guardium/guard_stap/guardctl --db-user=oracle --db-type=oracle --db-instance=oracle --db-home=
/dbarepzb/db/oracle/product/11.2.0.4 --db-version=11.2 store-conf
```

And

```
/opt/guardium/guard_stap/guardctl --db-instance=oracle authorize-user
```

2. Stop all Oracle processes. This ensures that `ORACLE_HOME` will still mount on primary.

3. Activate A-TAP on the primary node. For example:

```
/opt/guardium/guard_stap/guardctl --db-instance=oracle activate
```

4. Copy the `guard_tap.ini` file from the active node to all passive nodes, and change the `tap_ip` parameters appropriately. Then restart the S-TAP on the passive nodes.

5. Copy the A-TAP executer from the active node to all passive nodes. For example:

```
scp /opt/guardium/etc/guard/executor/root/* root@server:/opt/guardium/etc/guard/executor/root/
```

6. Restart the Oracle Services and verify that encrypted traffic is captured on the primary server.

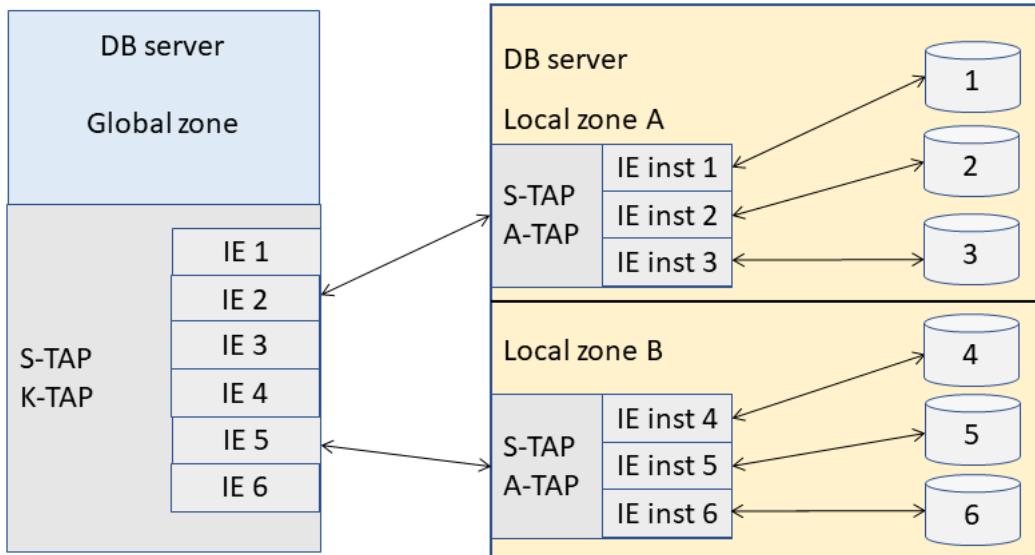
## Linux-UNIX: Installing and activating A-TAP in Solaris zones

---

Installing A-TAP in Solaris zones requires additional configuration.

### About this task

---



## Procedure

1. Install S-TAP/K-TAP on the global zone using GIM or shell installation and verify that inspection engines are configured for all local zones databases. If discovery did not find database instances running on the local zones, configure them manually for all available databases running in the local zones either in the `guard_tap.ini` file or the GUI.
2. In the local zone, install the same S-TAP version that is already installed in the global zone. (The S-TAP installer automatically detects the local zone environment and disables K-TAP by default).
3. Verify that inspection engines are configured in the S-TAPs in the local zones (installed in step 2) for all databases that require A-TAP. If discovery did not find database instances running on the local zones, manually create inspection engines for these databases using the `guard_tap.ini` file or the GUI.
4. Verify that the group ID (GID) for the group "guardium" is the same as the group ID for this group in the global zone. If the group IDs do not match, change the group ID in the local zones using command `groupmod -g <NEW_GID> guardium`. For example:

```
bash-3.2# groupmod -g 105 guardium
bash-3.2#
```

5. For each local zone where Oracle is installed, make sure the Guardium® device is mapped. Use these commands in the global zone environment.
  - a. Find the zone\_name by executing `zoneadm list`
  - b. `zoneadm -z <zone_name> halt`
  - c. `zonecfg -z <zone_name>`
  - d. `add device`
  - e. `set match=/dev/guard_ktap`
  - f. `end`
  - g. `verify`
  - h. For Solaris 11 devices `guard_ktap1`, `guard_ktap2`, `guard_ktap3`, `guard_ktap4`, `guard_ktap5`, repeat steps 5.d to g for each device. For example:

```
root@sys-sol11u3:~# zoneadm list
global
sys-sol11u3z2
sys-sol11u3z1
root@sys-sol11u3:~# zonecfg -z sys-sol11u3z2
zonecfg:sys-sol11u3z2> add device
zonecfg:sys-sol11u3z2:device> set match=/dev/guard_ktap
zonecfg:sys-sol11u3z2:device> end
zonecfg:sys-sol11u3z2> verify
zonecfg:sys-sol11u3z2> add device
zonecfg:sys-sol11u3z2:device> set match=/dev/guard_ktap1
zonecfg:sys-sol11u3z2:device> end
zonecfg:sys-sol11u3z2> verify
zonecfg:sys-sol11u3z2> add device
zonecfg:sys-sol11u3z2:device> set match=/dev/guard_ktap2
zonecfg:sys-sol11u3z2:device> end
zonecfg:sys-sol11u3z2> verify
zonecfg:sys-sol11u3z2> add device
zonecfg:sys-sol11u3z2:device> set match=/dev/guard_ktap3
zonecfg:sys-sol11u3z2:device> end
zonecfg:sys-sol11u3z2> verify
zonecfg:sys-sol11u3z2> add device
zonecfg:sys-sol11u3z2:device> set match=/dev/guard_ktap4
zonecfg:sys-sol11u3z2:device> end
zonecfg:sys-sol11u3z2> verify
zonecfg:sys-sol11u3z2> add device
zonecfg:sys-sol11u3z2:device> set match=/dev/guard_ktap5
zonecfg:sys-sol11u3z2:device> end
zonecfg:sys-sol11u3z2> verify
zonecfg:sys-sol11u3z2> exit
root@sys-sol11u3:~#
```

- i. For Solaris 10, the device names are different. To find the correct string for the devices, execute this command in the Global Zone environment:

```
ls /dev/ktap*|awk -F "-" '{print $1}'
```

Typical output looks like:

```
/dev/ktap_106844_0
/dev/ktap_106844_1
/dev/ktap_106844_2
/dev/ktap_106844_3
/dev/ktap_106844_4
/dev/ktap_106844_5
bash-3.2#
```

After mapping the devices, go to the relevant local zone dev directory and create links for mapped devices to /dev/guard\_ktap\*, for example:

```
bash-3.2# cd /zones/sol110z2/dev
bash-3.2# ln -fs ktap_106844_0 guard_ktap
bash-3.2# ln -fs ktp_106844_1 guard_ktp1
bash-3.2# ln -fs ktp_106844_2 guard_ktp2
bash-3.2# ln -fs ktp_106844_3 guard_ktp3
bash-3.2# ln -fs ktp_106844_4 guard_ktp4
bash-3.2# ln -fs ktp_106844_5 guard_ktp5
bash-3.2# ls -lrt *ktp*
crw-rw-rw- 1 root guardium 336, 5 Jul 15 12:36 ktp_106844_5
crw-rw-rw- 1 root guardium 336, 4 Jul 15 12:36 ktp_106844_4
crw-rw-rw- 1 root guardium 336, 3 Jul 15 12:36 ktp_106844_3
crw-rw-rw- 1 root guardium 336, 2 Jul 15 12:36 ktp_106844_2
crw-rw-rw- 1 root guardium 336, 1 Jul 15 12:36 ktp_106844_1
crw-rw-rw- 1 root guardium 336, 0 Jul 15 12:36 ktp_106844_0
lrwxrwxrwx 1 root root 13 Jul 19 10:58 guard_ktp -> ktp_106844_0
lrwxrwxrwx 1 root root 13 Jul 19 10:58 guard_ktp1 -> ktp_106844_1
lrwxrwxrwx 1 root root 13 Jul 19 10:59 guard_ktp2 -> ktp_106844_2
lrwxrwxrwx 1 root root 13 Jul 19 10:59 guard_ktp3 -> ktp_106844_3
lrwxrwxrwx 1 root root 13 Jul 19 10:59 guard_ktp4 -> ktp_106844_4
lrwxrwxrwx 1 root root 13 Jul 19 10:59 guard_ktp5 -> ktp_106844_5
```

j. Set the permissions so that `guard_ktp` and `ktp_xxxxx` are accessible by everyone, using the command: `chmod 0666 *ktp*`. For example:

```
bash-3.2# chmod 0666 *ktp*
```

#### k. exit

6. Verify that all devices are properly mapped by executing this command in the Global Zone environment:

```
zonecfg -z <zone_name> info|grep match
```

For example:

```
root@sys-sol11u3:~# zonecfg -z sys-sol11u3z2 info|grep match
match: /dev/guard_ktp4
match: /dev/guard_ktp3
match: /dev/guard_ktp2
match: /dev/guard_ktp1
match: /dev/guard_ktp
match: /dev/guard_ktp5
```

7. Boot the local zone by executing the command:

```
zoneadm -z <zone_name> boot
```

8. Note: A-TAP only needs to be activated in the global zone for encrypted databases running in the global zone. If required, activate it with the `guardctl` command option `activate`. It cannot be enabled with the encryption checkbox in the inspection engine section in GUI interface or by setting `encryption=1` in the `guard_tap.ini` file. If the database is not used on the global zone, then A-TAP activation in the global zone is not required. To activate A-TAP in the global zone, use the DB OS user. Activate A-TAP in the local zones using `guardctl`. Activation in local zones can only be performed by the root user with DB OS user authorization.

## Related reference

- [Linux-UNIX: guardctl utility commands for A-TAP](#)

## Linux-UNIX: Installing and activating A-TAP in WPARs environment

Installing A-TAP in WPARs requires additional configuration.

## About this task

### Procedure

- Install S-TAP/K-TAP in the AIX global environment using GIM or shell installation.
- In the WPAR, install the same S-TAP version that is already installed in the AIX global environment, with K-TAP disabled, since the kernel is shared in the WPAR.
- If discovery did not find database instances running on the WPAR, manually create inspection engines for these databases using `guard_tap.ini` or the GUI.
- Activate A-TAP using `guardctl` with user root. It cannot be done through enabling the encryption box in the inspection engine section in GUI interface or by setting `encryption=1` in the `guard_tap.ini` file. A-TAP (`guardctl`) activation may complain and issue warnings about errors installing libraries under `/usr/lib` (since that directory belongs to the AIX Global environment)
- Restart the S-TAP.

## Linux-UNIX: Deactivate and uninstall A-TAP in Zones and WPARs environment

## Procedure

---

1. On every sub-Zone/sub-WPAR with A-TAP installed/active:
  - a. Deactivate (and deinstrument if necessary, for Oracle on AIX) all A-TAPs using guardctl following the steps in [Linux-UNIX: Deactivating A-TAP](#).
  - b. Manually remove (`rm -rf`) the installation directory
  - c. Manually remove the ATAP libraries: `find /usr/lib -type f -name 'libguard-*.*' | xargs rm -f`

Note: Removing the libraries may give errors; these can be ignored.
2. Uninstall STAP/KTAP using the normal method
  - a. Remove the libraries: `find /usr/lib -type f -name 'libguard-*.*' | xargs rm -f o`
  - b. On Solaris, remove the ktap device from each zone's configuration:

```
zoneadm -z <zonenumber> halt
zonecfg -z <zonenumber>
<zonenumber>> info
```

If a ktap device is found, remove it:

```
<zonenumber> remove device match=/dev/ktap_xxxx (FOR SOLARIS 10)
<zonenumber> remove device match=/dev/guard_ktap (FOR SOLARIS 11)
<zonenumber>> verify
<zonenumber>> exit
zoneadm -z <zonenumber> boot
```
  - c. Remove the ktap device file and link from each sub-Zone/sub-WPAR device directory, for example:

```
/export/home2/zones/iris3/dev cd /export/home2/zones/iris3/dev
rm -f ktap_xxxx guard_ktap
```
  - d. With multiple KTAP devices, repeat the steps for each KTAP device by using the name ktap\_xxxx (Solaris 10) or guard\_ktap\_x (Solaris 11).

---

## Linux-UNIX: Upgrading A-TAP in Zones and WPARs environment

## Procedure

---

1. For Solaris Zone:
  - a. On the master/global-zone, remove the previously installed K-TAP device.

```
zoneadm -z <zonenumber> halt
zonecfg -z <zonenumber>
<zonenumber>> info
```
  - b. If a K-TAP device is found, remove it.

```
<zonenumber> remove device match=/dev/ktap_xxxx (for Solaris 10)
<zonenumber> remove device match=/dev/guard_ktap (for Solaris 11)

<zonenumber>> verify
<zonenumber>> exit
zoneadm -z <zonenumber> boot
```
  - c. For Solaris sub-zones, remove the previous K-TAP device file and link from sub-zone device directory. Go to the sub-zone device directory, for example `/export/home2/zones/iris3/dev`.

```
cd /export/home2/zones/iris3/dev
rm -f ktap_xxxx guard_ktap
```
2. For Solaris Zone:
  - a. On the master/global-zone, add the new K-TAP device to the zone configuration.

```
zoneadm -z <zonenumber> halt
zonecfg -z <zonenumber>
<zonenumber>> add device

<zonenumber>device> set match=/dev/ktap_xxxx (for Solaris 10)
<zonenumber>device> set match=/dev/ktap_xxxx (for Solaris 11)

<zonenumber>device> end
<zonenumber>> verify
<zonenumber>> exit
zoneadm -z <zonenumber> boot
```
  - b. Add the `guard_ktap` link and change permission. Go to the sub-zone device directory, for example: sub-zone device directory=`/export/home2/zones/iris3/dev`

```
cd /export/home2/zones/iris3/dev
ln -fs ktap_xxxx guard_ktap
chmod 0666 ktap_xxxx
chmod 0666 guard_ktap
```
  - c. Since there are multiple ktap devices, repeat steps for each K-TAP device by using the name ktap\_xxxx\_x(solaris 10) or guard\_ktap\_x (solaris 11)
3. For AIX WPARs: on WPARs, change permission on K-TAP devices. Go to the WPARs device directory, for example: wpar device directory=`/wpar/odin3/dev`

```
ln -fs ktap_xxxx guard_ktap
chmod 0666 ktap_xxxx
chmod 0666 guard_ktap
```

## Linux-UNIX: Configure and activate A-TAP steps for Teradata database

Step 1: Determine the user running gtwgateway and the path

For Example:

```
su11u1x64-tera:~ # ps -ef | grep gtwgateway
teradata 5000 4608 0 Jan03 ? 00:00:05 /usr/tgtw/bin/gtwgateway
root 20128 20063 0 12:35 pts/0 00:00:00 grep gtwgateway
```

gtwgateway runs as user teradata

Set parameter `--db-user=teradata` to guardctl

Path to gtwgateway is `/usr/tgtw/bin/gtwgateway`. This is the default value for the parameter `tdc_gtwgateway` and as such does not need to be specified.

Otherwise, the parameter should be `--tdc_gtwgateway=/usr/tgtw/bin/gtwgateway`

Step 2: Determine the path to pdemain

Typically, this will be `/usr/pde/bin/pdemain`

For Example:

```
su11u1x64-tera:~ # ps -ef | grep pdemain
root 4608 1 0 Jan03 ? 00:00:25 pdemain -debug
su11u1x64-tera:~ # ls -l /proc/4608/exe
lrwxrwxrwx 1 root tdtrusted 0 2015-01-03 01:20 /proc/4608/root 20620 20063
0 12:40 pts/0 00:00:00 grep pdemain/exe ->
/opt/teradata/tdat/pde/15h.00.00.07/bin/pdemain
```

Checking the inodes for this file and `/usr/pde/bin/pdemain`, we see that they are the same.

```
su11u1x64-tera:~ # ls -li /opt/teradata/tdat/pde/15h.00.00.07/bin/pdemain
1638875 -r-xr-xr-x 1 teradata tdtrusted 1294666 2014-01-22 01:40
/opt/teradata/tdat/pde/15h.00.00.07/bin/pdemain
su11u1x64-tera:~ # ls -li /usr/pde/bin/pdemain
1638875 -r-xr-xr-x 1 teradata tdtrusted 1294666 2014-01-22 01:40
/usr/pde/bin/pdemain
```

Since the inodes are the same and the default value for `--db-home=/usr/pde`, the parameter in this case does not need to be specified. Otherwise, you can specify `--db-home=/opt/teradata/tdat/pde/15h.00.00.07` or `--db-home=/usr/pde` since `bin/pdemain` in both paths is the same file hardlinked in this case.

Step 3: Stop the Teradata instance

For Example:

```
su11u1x64-tera:~ # /etc/init.d/tgtw stop
tgtw Shutdown complete
su11u1x64-tera:~ # /etc/init.d/tpa stop
PDE stopped for TPA shutdown
```

Step 4: Authorize the DB user to the Guardium group

For Example:

```
/usr/local/guardium/guard_stap/guardctl --db-instance=teradata authorize-user
```

Step 5: Store the configuration for A-TAP using the parameters determined in steps 1 and 2.

For Example:

```
/usr/local/guardium/guard_stap/guardctl --db-instance=teradata
--tdc_gtwgateway=/usr/tgtw/bin/gtwgateway --db-type=teradata
--db-home=/opt/teradata/tdat/pde/15h.00.00.07 --db-user=teradata store-conf
```

Step 6: Activate A-TAP

For Example:

```
/usr/local/guardium/guard_stap/guardctl --db-instance=teradata activate
```

#### Step 7: Restart the Teradata instance

For Example:

```
su11u1x64-tera:~ # /etc/init.d/tpa start
Teradata Database Initiator service is starting...
Teradata Database Initiator service started successfully.

su11u1x64-tera:~ # /etc/init.d/tgtw start
tgtw Startup complete
```

---

## Linux-UNIX: Oracle considerations for A-TAP

### A-TAP Procedure when working with Oracle Patch Installations

---

Oracle patches may invoke **relink** and will replace the Oracle executable, causing the A-TAP to stop functioning.

The correct procedure is:

1. Make sure all A-TAP instances are deactivated and deinstrumented.
2. Apply Oracle patch(es).
3. Instrument and activate all A-TAP instances

However, in case A-TAP was not properly deactivated prior to Oracle patch installation, DO NOT try to deactivate it after patch installation. Instead follow these steps:

1. Check if A-TAP IS OK.

```
grep guardium ${ORACLE_HOME}/bin/oracle >& /dev/null && echo "ATAP IS OK"

a. If ATAP IS OK is displayed, the A-TAP is still active and there is no need to do anything.
b. If ATAP IS OK is NOT displayed, remove ${ORACLE_HOME}/bin/oracle-guard and activate the A-TAP.
```

In case everything else fails:

- Remove \${ORACLE\_HOME}/bin/oracle-guard
- Run **relink all**

### A-TAP Problems And Solutions associated with Oracle Permissions

---

Several problems may occur that have to do with user and group permissions.

- In 'BEQUEATH' access from the user other than the one that installed the database the permissions have to be set manually:
  - add user running sqlplus to group 'guardium'
  - open the read permissions 'chmod a+r' on the following two directories:  

```
/usr/local/guardium/xxx/etc/guard
/usr/local/guardium/xxx/etc/guard/executor
```

    - make sure that the SUID and SGID bits are on \${ORACLE\_HOME}/bin/oracle.
      - If not, run the command **chmod ug+s \${ORACLE\_HOME}/bin/oracle**
- If the UID or EUID are not members of OWNER group GID, the reason for permission denied is that the user matching UID or EUID does not belong to group matching OWNER GID.
- To make it easier, not having to handle different OS syntaxes for adding users and groups, while disabling the automatic addition to group Guardium, two commands are available within guardctl which can be used irrespective of the method you use to activate ATAP (i.e. guardctl or guard\_tap.ini):
  - #/path/to/guardium/bin/guardctl is-user-authorized
  - #/path/to/guardium/bin/guardctl authorize-user ...

Note: Group Guardium can be removed on most OS's with **groupdel guardium**. However, after removal, only the **guard\_ktap\_loader** parameter can correctly re-create it and change the K-TAP device permissions.

---

## Linux-UNIX: Troubleshooting A-TAP configuration issues

This section summarizes common mistakes made during A-TAP configurations, their symptoms, and how to avoid them.

Table 1. A-TAP configuration issues and recommendations

| Symptoms                                        | Mistake                                                          | Platform | How to Avoid                                                                                                                                                  |
|-------------------------------------------------|------------------------------------------------------------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Activation command fails.                       | Wrong db_home parameter                                          | All      | Verify that the value of db_home is correct.                                                                                                                  |
| Activation command fails.                       | OS user logged in                                                | All      | Always make sure the OS user is not logged in. Use w command to see which users are logged in.                                                                |
| 12.1 Activation fails for Oracle Database 23ai. | Activating A-TAP with wrong parameters for Oracle Database 23ai. |          | Before you activate A-TAP, set the following parameters: <ul style="list-style-type: none"><li>• db_version = 23</li><li>• db_use_instrumented = no</li></ul> |

| Symptoms                       | Mistake                                | Platform | How to Avoid                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------|----------------------------------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Database does not start.       | Wrong instance name                    | All      | Verify the db_instance name is specific correctly.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Traffic is not logged.         | Wrong or missing db_version            | AIX      | Always specify numeric version (for example, 10.2 or 9.2). The version number can have only one digit after the decimal point. For Db2: Verify that the IE configuration is correct. Run the script <b>find_db2_shmem_parameters.sh</b> , located under <code>stap_directory/bin</code> . Execute it either as root or Db2 user, using the db2 instance name as a parameter. It returns the shared memory parameters, including Db2 shared memory size, Client position and header size. Verify that the IE parameters defined in Guardium match these returned values. |
| Fails to activate.             | Missing Oracle-guard-instrumented      | AIX      | Instrument command must be run first to create a re-linked instrumented Oracle executable                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Error during A-TAP activation. | Insufficient disk space, install exits |          | Clean up disk space and retry. If that does not help, change db_space=8 to db_space=1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Linux-UNIX: Configure a public and private address for an S-TAP

For an S-TAP deployed in a private network, Guardium® can refer to the S-TAP with a public IP address that is not visible from the database server on which S-TAP is installed, while the database uses a private address for the S-TAP.

### About this task

Typical scenarios where the Guardium system cannot recognize the S-TAPs IPs, and the IPs that can be validated by system are not the IPs you want to report data with:

- Cloud deployment with internal and external IPs.
- S-TAP clients are using private IPs, for example when running OpenStack and creating VMs.

You can modify the S-TAP configuration in the:

- S-TAP Control page, Details section: Force server IP
- Manage > Module Installation > Set up by Client page.
- S-TAP configuration file `guard_tap.ini`: `force_server_ip`.

For example, you create a database system in the cloud. Internal to that system (if you're logged in), the server identifies with the IP address 1.1.1.1. But from the outside world (from any other machine), it responds to the IP 2.2.2.2. This makes it difficult to identify servers in report. If you set the `tap_ip` to 2.2.2.2, and set the `private_tap_ip` to 127.0.0.1 (default if it is a local IP), everything works smoothly, but there are inconsistencies between reports. To resolve this, set `force_server_ip=1`, then the server only identifies with the external, public IP (TAP IP), and all reports from this database use the IP 2.2.2.2 (one single consistent IP address).

### Procedure

- Specify `tap_ip` in the `guard_tap.ini`, or `STAP_TAP_IP` in the Set up by Client page to the external, public IP address (virtual IP). This is the IP reported as the S-TAP host in the S-TAP Control page. If `tap_ip` is set to a name, it has to be resolvable by `getservername()`.
- Specify `private_tap_ip` in the `guard_tap.ini`, or `STAP_PRIVATE_TAP_IP` in the Set up by Client page, to an IP address that the database host can recognize (physical IP).
- Optional: If you want the collector to record the server IP address to be the address specified in `tap_ip`, set `force_server_ip=1` in the `guard_tap.ini`, or `STAP_FORCE_SERVER_IP` in the Set up by Client page or from the S-TAP Control page, Details section.

### Results

When the S-TAP registers with the collector, the S-TAP appears as having the external IP address.

### Related tasks

- [Set up by Client](#)

## Linux-UNIX: Configure S-TAP log and dump locations when /root partition size is limited

S-TAP agents are installed in a partition with root privileges; by default they are installed into the `/root` partition based directories. For customers with limited root file systems size, follow these best practice recommendations to prevent the S-TAP agent from generating logs or dumps on the `/root` partition.

### Procedure

- Redirect the S-TAP debug log to a partition whose size is larger than `/root`. By default the S-TAP log writes to the `/tmp` directory. Change the write directory using one of the following:
  - Use the GuardAPI command `update_stap_config`. This example redirects the logs to `/var`: `xxx.xxx.xxx.com> grdapi update_stap_config stapHost=xxxx updateValue=TAP.tap_log_dir:/var`
  - In the `guard_tap.ini` file, change the parameter `tap_log_dir` value to the new target directory. For example, `tap_log_dir=/var`. Restart the S-TAP.
- Redirect the core dumps to a partition outside of `/root` that is larger in size. (By default the cores are generated in the `<guard install dir>`.) On Linux systems:

- a. Open the file /etc/abrt/abrt.conf
  - b. Set DumpLocation = <desired location>
  - c. Restart the service with: **restart abrt.service**
3. Rotate the log files using one of the following options:
- Use the guard\_monitor tool that is part of Guardium S-TAP agent to redirect and rotate Guardium logs. See:[Linux-UNIX: S-TAP Monitor \(guard\\_monitor\)](#). Specifically, use these parameters:

```
; maximum file size of monitor log file (KB)
monitor_log_rotate_size=1024
; number of rotated monitor logs to keep
monitor_log_rotate_num_kept=5
; maximum file size of log files (KB)
log_rotate_size=4096
; number of rotated logs to keep
log_rotate_num_kept=5
; logs to rotate
logs_to_rotate=/tmp/guard_stap.stderr.txt,/tmp/guard_stap.stdout.txt,/usr/local/guardium/guard_stap/ktap/ktap_install.log,/usr/local/guardium/guard_stap/guard_discovery.stderr.log
```

Note:

Set logs\_to\_rotate to include any redirected log files as described in [1](#). For example, if you redirected logs to /var, then logs\_to\_rotate would be:logs\_to\_rotate=/var/guard\_stap.stderr.txt,/var/guard\_stap.stdout.txt,/usr/local/guardium/guard\_stap/ktap/ktap\_install.log

On some OS other log files may get used and can therefore be included for rotation. For example:

```
logs_to_rotate=/tmp/guard_stap.stderr.txt,/tmp/guard_stap.stdout.txt,/var/log/ktap_install.log,/opt/guardium/guard_stap/guard_discovery.stderr.log,/var/log/ktap.log,/var/guard_stap.stderr.txt,/var/guard_stap.stdout.txt,/usr/local/guardium/guard_stap/ktap/ktap_install.log,/usr/local/guardium/guard_stap/guard_discovery.stderr.log,/var/tmp/ktap-trace.txt
```

- Use the Unix native Log rotation **logrotate** or any comparable software, to manage logs on the DB server.

## Linux-UNIX: Editing the S-TAP configuration parameters

You can modify the S-TAP configuration after it is installed using GIM, the UI, or for advanced users, the configuration file on the database.

Note: Parameters in the GUI may be safely changed. Parameters that are not in the GUI are advanced, and rarely need changing. They are for use by Guardium support or advanced users.

**CAUTION:**

Do not modify advanced parameters unless you are an expert user or you have consulted with IBM Technical Support.

You can some modify parameters in the GUI. See [Linux-UNIX: Configuring S-TAP in the S-TAP Control page](#).

GIM is an easy method for modifying parameters, if the S-TAP bundle was installed with GIM. See [Set up by Client](#).

Configuration Change Alerting: When the S-TAP sends an updated configuration to the collector, the collector checks the new configuration against the last stored configuration on the collector and an alert is generated detailing what has changed. This alert appears in the S-TAP event log. If a section is added or removed, the parameters of that section are listed. If a section parameter is changed, it displays the section name, parameter name, old value, and new value. If a parameter is added or removed from a section, the section name, parameter name, and value are displayed. For example:  

```
UTAP 'rh7-docker1' configuration changed,
differences: Section 'TAP' parameter
'discovery_debug' changed from '0' to '1' Section 'TAP' parameter 'stap_statistic' changed from '1'
to '0' Section 'SQLGuard_1' added Section 'SQLGuard_1' parameter 'connection_pool_size'='0' added
Section 'SQLGuard_1' parameter 'num_main_thread'='1' added Section 'SQLGuard_1' parameter
'primary'='2' added Section 'SQLGuard_1' parameter 'sqlguard_ip'='gimb39' added Section 'SQLGuard_1'
parameter 'sqlguard_port'='16016' added
```

If it is necessary to modify the configuration file from the database server, follow the procedure described in this section. The guard\_tap.ini file contains comments that explain many of the parameters.

The S-TAP needs restarting after you modify the guard\_tap.ini file. Either restart it in the S-TAP Control page with the [Send command](#) or using one of: [Linux-UNIX: Start and stop S-TAP and GIM processes for various OS types/versions](#), [Linux-UNIX: Using guard-config-update to start, restart, and stop S-TAP, and view status](#).

The guard\_tap.ini file has a [Proxy] section that is only used for the Guardium External S-TAP containers. Do not modify any parameters in this section.

**CAUTION:**

Parameters must be added to their relevant section: [TAP], [SQLGuard], [DB\_<name>].

1. Log on to the database server system using the root account.
2. Stop the S-TAP.
3. Make a backup copy of the configuration file: guard\_tap.ini. The default file locations is /usr/local/guardium/guard\_stap/guard\_tap.ini
4. Open the configuration file in a text editor.
5. Edit the file as necessary.
6. Save the file.
7. Restart the S-TAP and verify that your change has been incorporated.

- [Linux-UNIX: Guardium Hosts \(SQLGuard\) parameters](#)

These parameters describe a Guardium system to which this S-TAP can connect. All parameters in this section are basic, and appear in the [SQL\_GUARD] section.

- [Linux-UNIX: General parameters](#)

These parameters define basic properties of the S-TAP running on a database server and the server on which it is installed, and do not fall into any of the other categories.

- [Linux-UNIX: Inspection engine parameters](#)

These parameters affect the behavior of the inspection engine that the S-TAP uses to monitor a data repository on a DB server.

- [Linux-UNIX: Oracle Unified Auditing parameters](#)

These parameters define the Oracle Unified Auditing connection between the S-TAP and the SQL server.

- [Linux-UNIX: Firewall parameters](#)

These parameters affect the behavior of the S-TAP with respect to the firewall.

- [Linux-UNIX: Query rewrite parameters](#)

The query rewrite parameters affect the behavior of the S-TAP with respect to discovery.

- [Linux-UNIX: Server-side masking \(SSM\) parameters](#)  
The server-side masking parameters affect the behavior of the S-TAP with respect to discovery.
- [Linux-UNIX: Discovery parameters](#)  
The discovery parameters define the behavior of the auto-discovery feature, for discovering database instances and sending the results to the current active S-TAP.
- [Linux-UNIX: Application server parameters](#)  
These parameters affect the behavior of the S-TAP when an application user name needs to be bounded with database activities.
- [Linux-UNIX: Hadoop parameters](#)  
Guardium supports Hadoop integration using HDFS, Hortonworks with Apache Ranger, and Cloudera Navigator. Understand the S-TAP configuration required for these integrations.
- [Linux-UNIX: Configuration Auditing System \(CAS\) parameters](#)  
These parameters affect the behavior of CAS.
- [Linux-UNIX: Debug parameters](#)  
These parameters affect the behavior of S-TAP debugging.
- [Linux-UNIX: K-TAP parameters](#)  
These parameters affect the behavior of the K-TAP.

## Linux-UNIX: Guardium Hosts (SQLGuard) parameters

These parameters describe a Guardium system to which this S-TAP can connect. All parameters in this section are basic, and appear in the [SQL\_GUARD] section.

| GUI                                                                        | GIM              | guard_tap.ini        | Default value | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------|------------------|----------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pool size                                                                  |                  | connection_pool_size | 0             | The number of connections to open between the S-TAP and the sniffer process on a Guardium® host. Increasing the value provides more throughput that might be required when encryption such as TLS is enabled. The maximum number of pooled connections is 50. The total is the sum of (connection_pool_size x num_main_thread) in all of the [SQLGuard_n] sections in the guard_tap.ini.<br>Valid values: <ul style="list-style-type: none"><li>• 0: Disable pooling</li><li>• 1-10: (for each defined host)</li></ul> |
| Main threads                                                               |                  | num_main_thread      | 1             | The number of threads that are used between the S-TAP and a Guardium host.<br>Valid values: 1-10 (maximum total of 10 for all defined Guardium hosts)<br>Note: Enterprise load balancing does not support multiple threads for a single managed unit. Set this parameter to 1 if you are using enterprise load balancing.                                                                                                                                                                                              |
| <input checked="" type="checkbox"/> (checkmark indicates the primary host) |                  | primary              |               | Indicates the primary Guardium system for this S-TAP. In guard_tap.ini: 1=Primary, 2=Seconday, 3=tertiary, and so on                                                                                                                                                                                                                                                                                                                                                                                                   |
|                                                                            |                  | sqlguard_port        | 16016         | Read only. Port used for S-TAP to connect to Guardium system.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Guardium Host                                                              | STAP_SQLGUARD_IP | sqlguard_ip          | NULL          | IP address or hostname of the Guardium system that acts as the host for the S-TAP. You can define multiple hosts by adding sections [SQLGuard_1], [SQLGuard_2], and so on.                                                                                                                                                                                                                                                                                                                                             |

## Linux-UNIX: General parameters

These parameters define basic properties of the S-TAP running on a database server and the server on which it is installed, and do not fall into any of the other categories.

These parameters are stored in the [TAP] section of the S-TAP properties file. **DB2\_SHMEM\_DRIVER\_INSTALLED**

Table 1. S-TAP configuration parameters in the [TAP] section

| GUI             | GIM         | guard_tap.ini                                   | Default value | Description                                                                                                                                                                                                     |
|-----------------|-------------|-------------------------------------------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 |             | ranger_hdfs_audit_history_length                | 30            | Length of the audit history<br>Valid values range = -24 to 60. The negative integers are hours and positive integers are days.<br>Valid value = 0 means that S-TAP reads the audits from the beginning of time. |
|                 |             | stap_buf_mem_percent                            | 30            | If there is no allow the memory specified for the stap process, calculate percentage of total memory used for stap ring buffer<br>Valid values: 1 - 100.                                                        |
|                 |             | tap_disable_intercept_after_x_missed_heartbeats | 0             | Valid values: 0 - 100.                                                                                                                                                                                          |
|                 |             | tap_type                                        |               | The type of installed S-TAP agent: <ul style="list-style-type: none"><li>• stap=UNIX</li><li>• ztap=Z/OS</li></ul>                                                                                              |
| Version         |             | tap_version                                     |               | Read only. The S-TAP version that is installed on the DB server, added to the file during installation or upgrade only.                                                                                         |
| S-TAP Host      | STAP_TAP_IP | tap_ip                                          |               | Read only. IP address or hostname for the database server system on which S-TAP is installed.                                                                                                                   |
| Force server IP |             | force_server_ip                                 | 0             | Forces the reported server IP of database to be the value stored in tap_ip. Valid values: <ul style="list-style-type: none"><li>• 0: Disabled</li><li>• 1: Enabled</li></ul>                                    |

| GUI             | GIM                                | guard_tap.ini                 | Default value | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------|------------------------------------|-------------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Private tap IP  |                                    | private_tap_ip                |               | If this parameter is defined, the database uses it for the S-TAP communication. (Relevant when the S-TAP is deployed in a private network; the external, public IP address of the S-TAP is defined by tap_ip. See <a href="#">Linux-UNIX: Configure a public and private address for an S-TAP</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Devices         | STAP_DEVICES                       | devices                       | none          | Which interfaces to listen on. Use <b>ifconfig</b> to find the correct interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| All can control | STAP_ALL_CAN_CONTROL               | all_can_control               | 0             | Defines which Guardium system control this S-TAP. Valid values: <ul style="list-style-type: none"> <li>• 0: S-TAP is controlled by the primary Guardium system only.</li> <li>• 1: S-TAP can be controlled by any Guardium system.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Load balancing  | STAP_PARTICIPATE_IN_LOAD_BALANCING | participate_in_load_balancing | 0             | Controls S-TAP load balancing (not enterprise load balancing) to Guardium systems. Valid values: <ul style="list-style-type: none"> <li>• 0: No load balancing.</li> <li>• 1: Load balancing. Traffic is balanced between the primary and secondary servers, which are defined in the SQLGuard section.</li> <li>• 2: Redundancy. Fully mirrored S-TAP sends all traffic to all primary and secondary servers, which are defined in the SQLGuard section.</li> <li>• 3: Hardware load balancing. Guardium uses a load balancer such as F5 or Cisco. S-TAP sends the traffic to the load balancer, which forwards it to one of the collectors in the pool.</li> <li>• 4:S-TAP is configured for multi-threading. Set NUM_MAIN_THREAD from 0 to 10.</li> </ul> <p>Use the primary parameter in the SQLGUARD section to specify primary, secondary (and so on), servers. If this parameter is set to 0, and you have more than one Guardium system monitoring traffic, then the non-primary Guardium systems are available for failover.</p> |
|                 |                                    | initial_balancer_tap_group    |               | The S-TAP group name to associate with this S-TAP (by the central manager load balancer) when installing an S-TAP. The group name is sent with each request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                 |                                    | initial_balancer_mu_group     |               | The managed unit group name to associate with this S-TAP (by the central manager load balancer) when installing an S-TAP. The group name is sent with each request.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                 |                                    | external_load_balancing       | 1             | To use an S-TAP with Guardium Insights, this parameter must be set to 1, which sets load balancing for the Guardium Insights connections.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                 | TENANT_ID                          | tenant_id                     |               | To use an S-TAP with Guardium Insights, the Guardium Insights tenant ID is required, including the TNT_ prefix. For example:<br><b>tenant_id=TNT_N5YBRAFBWRYAPFLQWABCDE</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                 | STAP_CONNECTION_TIMEOUT_SEC        | connection_timeout_sec        | 10            | Number of seconds after which the S-TAP considers a Guardium server to be unavailable. It can have any integer value. Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                 | STAP_USE_EXIT_DB_TYPE              | use_exit_db_type              | 0             | Allows database auto-discovery to discover any databases that have Exit protocols and add those instances to Discovered Instances report.<br>Valid values: <ul style="list-style-type: none"> <li>• 0: Do not autodiscover databases that have Exit protocols.</li> <li>• 1: Discover databases that have Exit protocols. For more information, see <a href="#">Using Exit discovery</a>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                 | STAP_DB_EXIT_LIST                  | db_exit_list                  | All           | Discover databases that are supported with Exits. When an Exit database type is discovered, K-TAP is automatically disabled.<br><br>When <b>use_db_exit</b> is set to 0, this parameter is ignored.<br><br>Valid values (when <b>use_db_exit</b> is set to 1): <ul style="list-style-type: none"> <li>• All - Discovery discovers databases supported with Exit along with other non-Exit databases.</li> <li>• None: Discovery does not discover any databases with Exits.</li> <li>• &lt;DB type&gt; : Discovery discovers only the specified database. DB type can be: DB2, INFORMIX, NETEZZA, or TERADATA.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                 |
| TLS Use         | STAP_USE_TLS                       | use_tls                       | 0             | Use SSL to encrypt traffic between the S-TAP and the Guardium appliance. Valid values: <ul style="list-style-type: none"> <li>• 0: Do not encrypt. <b>The traffic between the agent and Guardium system is in clear text.</b></li> <li>• 1: Use SSL to encrypt traffic between the agent and the Guardium system. This adds ~15% of CPU usage to the sniffer's S-TAP server but does not affect the sniffer's other modules.</li> </ul> <p>Guardium recommends encrypting network traffic between the S-TAP and the collector whenever possible: only in cases where the performance is a higher priority than security should this be disabled.</p> <p>Can be set when pushing to a group of DB servers via GIM.</p>                                                                                                                                                                                                                                                                                                                     |
| TLS Failover    | STAP_FAILOVER_TLS                  | failover_tls                  | 0             | Deprecated in v10.5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| GUI                  | GIM                   | guard_tap.ini               | Default value | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------|-----------------------|-----------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Wait for DB exec     | STAP_WAIT_FOR_DB_EXEC | wait_for_db_exec            | 0             | <p>When S-TAP restarts, either from a system reboot or user initiated S-TAP stop / start commands, S-TAP polls all databases that have been configured to be monitored and begins monitoring all valid configurations. Any configuration anomalies (either on the database side or the S-TAP side) that limits S-TAP ability to monitor a database does not limit the S-TAP from monitoring other databases with valid configurations. This parameter determines the S-TAP response, and its status in the S-TAP Control page, if a DB instance is not available (db_install_dir or db_exec_file is not accessible) during IE validation, after an S-TAP or DB restart. Valid values:</p> <ul style="list-style-type: none"> <li>• 0 and less: S-TAP logs an event message with the event type CONF_ERROR when a DB instance is detected as unavailable for certain DB(PROTOCOL) during the S-TAP starting time. S-TAP also logs a CONF_ERROR if a DB changes its status from available to unavailable during the periodic check (every 15 minutes). These event messages change the S-TAP status in the GUI to yellow with the instruction to correct the parameter or set WAIT_FOR_DB_EXEC &gt; 0. When a DB instance status changes from unavailable to available, a WARNING message is sent to the sniffer, but the GUI status does not change automatically. You need to click  to open the S-TAP event log and click Accept.</li> <li>• greater than 0: A WARNING is logged for any unavailable database during S-TAP startup time or during a periodic check. The time interval of the periodic check is the value of wait_for_db_exec, in minutes. A warning message is also sent when an unavailable DB instance becomes available. Since the periodic check needs to get status of the database file configured for each inspection engine, and it consumes the CPUs, the value should not be less than the number of inspection engines.</li> </ul> <p>See <a href="#">Linux-UNIX: Configuring S-TAP in the S-TAP Control page</a> for more details on the S-TAP Status page. Before setting this property to a positive value, be sure to set all other necessary configuration properties and test that the S-TAP starts and collects data correctly. This property can be modified using GIM GUI (STAP_WAIT_FOR_DB_EXEC), and the guard_tap.ini configuration file.</p> |
| Dynamic ring buffers |                       | enable_dynamic_ring_buffers | 0             | <p>Dynamically adds and removes S-TAP buffers for each main connection during peak traffic, to prevent an overflow in the S-TAP buffer. If S-TAP failover happens, data in all buffers is moved to the new buffers.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Disabled</li> <li>• 1: Enabled</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|                      | STAP_RUN_AS_ROOT      | tap_run_as_root             | 1             | <p>Run S-TAP as user root or as user guardium. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Run as guardium user</li> <li>• 1: Run as root</li> </ul> <p>In some cases you need to run the S-TAP as guardium (and not root). This can cause other issues and should only be used when necessary. Running S-TAP as the guardium user can cause a database or protocol to stop working because of permission levels. Verify that the database path or exec file gives the Guardium user read permission. Depending on your environment, typical limitations are:</p> <ul style="list-style-type: none"> <li>• <b>wait_for_db_exec</b> might not work. For cluster, check the database path or exec file for Guardium user read permission.</li> <li>• Database on AIX® WPAR and Solaris Zones may not work, check the permission to access the install path or exec file</li> <li>• For Oracle BEQ, restart S-TAP after starting or restarting the database.</li> <li>• For Informix® shared memory, restart S-TAP after starting or restarting the database.</li> <li>• For DB2 shared memory, if <b>shmctl</b> failed because of permission issue, then in most cases S-TAP should be changed to run as root. <ul style="list-style-type: none"> <li>◦ If shared memory segment has read permission by group, then make sure the DB2 instance has been added to user (Guardium) group. But still on each server, only one set of configuration of DB2® can be supported.</li> <li>◦ If shared memory segment has read permission by db2 user only, then S-TAP has to run as root. (open a DB2 shared memory session, run command <b>ipcs -ma</b>, check MODE on the output)</li> </ul> </li> </ul> <p>Can be set when pushing to a group of DB servers via GIM.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                      | STAP_TAP_BUF_DIR      | tap_buf_dir                 | NULL          | Location of S-TAP buffer file if S-TAP is using map file. Default location is \$inidir/buffers<br>Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                      | STAP_TAP_LOG_DIR      | tap_log_dir                 | NULL          | Location of S-TAP log files: guard_stap.stdout.tx, guard_stap.stderr.txt, guard_stap.fam.txt. By default, log files are written in /tmp.<br>Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Alternate ips        | STAP_ALTERNATE_IPS    | alternate_ips               | NULL          | Additional IP addresses for the database server system on which the S-TAP is installed. If there are no additional IP addresses, enter the property exactly as shown (with no values).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|                      |                       | tee_msg_buf_len             | 128           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                      | STAP_BUFFER_FILE_SIZE | buffer_file_size            | 50            | Advanced. Size in MB of the buffer allocated for the packets queue. If the buffer size is set too large, the S-TAP might not be able to start. Maximum size is 2000MB.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

| GUI                       | GIM                               | guard_tap.ini                         | Default value | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------|-----------------------------------|---------------------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                           | STAP_BUFFER_MMAP_FILE             | buffer_mmap_file                      | 0             | <p>How to map S-TAP and Guardium system communication buffer. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Use an anonymous file</li> <li>• 1: Use an mmap file</li> </ul> <p>Can be set when pushing to a group of DB servers via GIM.</p>                                                                                                                                                                                                                                                  |
|                           | STAP_BUF_MSG_TIME_INTERVAL        | buf_msg_time_interval                 | 5             | Interval, in minutes, to log S-TAP buffer overflow message. Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                                                                                                                                                                                                                         |
|                           |                                   | buffer_percentage_for_priority_packet | 1             | <p>Allows you to adjust the buffer percentage for priority packets. Increasing the value reserves more space for priority packets.</p> <p>When Guardium reaches the buffer usage maximum (that is, 100% - buffer_percentage_for_priority_packet), non-priority packets are dropped to help ensure that priority packets get through.</p> <p>The range is 1 (1%, the default) to 5 (5%).</p>                                                                                                                   |
|                           |                                   | transmit_session_losses_metadata      | 1             | <p>Determines whether to create a SessionLossesMetadata message that report metadata if packets are dropped for a given session.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>• 0 (disabled). Do not send the SessionLossesMetadata message.</li> <li>• 1 (enabled). Send the SessionLossesMetadata, but only when a new collector is found.</li> </ul>                                                                                                                                    |
| Trace files dir           |                                   | tracefiles_dir                        |               | The directory in which access tracer files are stored.                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Compres. Level            | STAP_COMPRESSION_LEVEL            | compression_level                     | 0             | <p>Increase the compression level to lower the number of bytes between the S-TAP and the collector. Changing the compression level is recommended where latency is high between the data centers, to reduce travel time. Compression might impact performance on both ends (S-TAP and collector (sniffer)). The disk usage is not affected by compression. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: No compression</li> <li>• 1: Best speed</li> <li>• 9: Highest compression</li> </ul> |
|                           | STAP_MIN_BYTES_TO_COMPRESS        | min_bytes_to_compress                 | 500           | Advanced. Minimum number of bytes to compress when compression is enabled. Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                                                                                                                                                                                                          |
|                           | STAP_TAP_MIN_HEARTBEAT_INTERVAL   | tap_min_heartbeat_interval            | 20            | Maximum time the S-TAP attempts to write to the primary Guardium system buffer before attempting to write to the secondary Guardium buffer. Also see connection_timeout_sec for S-TAP failover to secondary collector. Should be greater than or equal to connection_timeout_sec. Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                   |
|                           | STAP_MSG_AGGREGATE_TIMEOUT        | msg_aggregate_timeout                 | 100           | Time interval, in milliseconds, for K-TAP packets to aggregate before notifying S-TAP of ready data. Can be any integer value. Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                                                                                                                                                      |
|                           | STAP_MSG_COUNT_WATERMARK          | msg_count_watermark                   | 64            | Maximum number of KTAP packets to aggregate before notifying S-TAP of ready data. Can be any integer value. Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                                                                                                                                                                         |
|                           | STAP_LOG_PROGRAM_NAME             | log_program_name                      | 0             | <p>Controls sending source program name to the Guardium system. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Don't send <code>source_program</code> name.</li> <li>• 1: Send <code>source_program</code> name.</li> </ul> <p>When enabled, can boost performance, but you can't tell which program name was using the connection (though all other connection information like user and client address are available). Can be set when pushing to a group of DB servers via GIM.</p>         |
|                           | STAP_MAX_SERVER_WRITE_SIZE        | max_server_write_size                 | 65536         | The maximum number of bytes that the S-TAP sends to the Guardium system at once. Can be any integer value. Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                                                                                                                                                                          |
|                           |                                   | guardium_ca_path                      | NULL          | Location of the Certificate Authority certificate.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                           |                                   | sqlguard_cert_cn                      | NULL          | The common name to expect from the Sqlguard certificate.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                           |                                   | guardium_crl_path                     | NULL          | The path to the Certificate Revocation list file or directory.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|                           | STAP_TAP_FAILOVER_SESSION_SIZE    | tap_failover_session_size             | 1024          | <p>The maximum number of entries in the session failover file per Guardium system. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Failover feature is disabled.</li> <li>• Positive integer: Number of retries</li> </ul> <p>Can be set when pushing to a group of DB servers via GIM.</p>                                                                                                                                                                                                     |
|                           | STAP_TAP_FAILOVER_SESSION QUIESCE | tap_failover_session_quiesce          | 240           | Time, in seconds, to keep failover session info after failover. After this time interval, unused sessions in the failover list from the previous active servers are removed from the current active server, including cleaning the sessions' policies and removing the sessions from the firewalled and scrubbed lists. Can be set when pushing to a group of DB servers via GIM.                                                                                                                             |
| Kerberos plugin directory | STAP_KERBEROS_PLUGIN_DIR          | kerberos_plugin_dir                   | NULL          | The Kerberos plugin file location.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| GUI | GIM                               | guard_tap.ini                         | Default value   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----|-----------------------------------|---------------------------------------|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     | STAP_DB_IGNORE_RESPONSE           | db_ignore_response                    | NULL            | <p>Responses from the database include result sets, database exceptions (such as SQL errors), and failed login messages. If you do not need to monitor all responses, use this parameter to configure which DB types are response-ignored. db_ignore_response starts when the session traffic reaches the threshold db_ignore_response_bypass_bytes. Valid values:</p> <ul style="list-style-type: none"> <li>• none: No response is ignored</li> <li>• all: The responses from all DBs are ignored</li> <li>• Comma-separated list of DB types to be response-ignored, for example: MYSQL,DB2</li> </ul> <p>Note: If using db_ignore_response=all to set the Oracle database response to be ignored (not captured to reduce traffic load), then be aware that more than just database server responses are involved. Database server responses can also contain important database protocol metadata information used by the application for following database requests interpretation. For example, Login Failed and SQL Exceptions.</p> |
|     | STAP_STATISTIC                    | stap_statistic                        | 0               | <p>Interval at which S-TAP sends statistic information about S-TAP/K-TAP to sniffer. Valid values:</p> <ul style="list-style-type: none"> <li>• Positive integer: Number of hours</li> <li>• Negative integer: Number of minutes</li> <li>• 0: Do not send</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|     |                                   | stap_statistic_version                | 1               | S-TAP statistics are version-specific to the collector. Valid values: <ul style="list-style-type: none"> <li>• 0: Guardium V9</li> <li>• 1: Guardium V10 and higher</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|     | STAP_UPLOAD_FEATURE               | upload_feature                        | 1               | Whether or not the S-TAP uploads snapshots and new K-TAP modules to the GIM server to which it reports. Valid values: <ul style="list-style-type: none"> <li>• 0: Disabled</li> <li>• 1: Enabled for all (snapshots and K-TAP modules)</li> <li>• 2: Enabled for snapshot; disable for K-TAP modules</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|     | STAP_UPLOAD_SNAPSHOTS             | upload_snapshots                      | 1               | Controls automatic upload of snapshots using the file upload mechanism. Valid values: <ul style="list-style-type: none"> <li>• 0: Disabled</li> <li>• 1: Enabled</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|     |                                   | add_to_verification_schedule          | 0               | Add the Inspection Engines defined in guard_tap.ini to the S-TAP Verification schedule. S-TAP verification tests traffic capture. Valid values: <ul style="list-style-type: none"> <li>• 0: Disabled</li> <li>• 1: Enabled</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|     | STAP_DB_IGNORE_BY_BYPASS_BYTES    | db_ignore_response_bypass_bytes       | 4096            | db_ignore_response starts when bypass bytes are reached. Relevant only if db_ignore_response is set to all, or is not set to none.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|     | STAP_DB_IGNORE_RESETS_PER_REQUEST | db_ignore_response_resets_per_request | 0               | Specifies when the db_ignore_response restarts its counter. Valid values: <ul style="list-style-type: none"> <li>• 0: The total length is counted for all client-to-server packets, starting with the first packet of the session.</li> <li>• 1: Count restarts after every client-to-server packet (reset per session).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|     | STAP_DB_IGNORE_RESPONSE_FILTER    | db_ignore_response_filter             | 0.0.0.0/0.0.0.0 | Comma separated list of IP/MASKs to be response-ignored. By default it filters all TCP traffic. Any DB responses of the type specified by db_ignore_response to the specified IP/MASKs are ignored. Valid values: <ul style="list-style-type: none"> <li>• 0: No filtering of responses occurs</li> <li>• 0.0.0.0/0.0.0.0: All IPs are filtered</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|     | STAP_DB_IGNORE_RESPONSE_LOCAL     | db_ignore_response_local              | 1               | Filtering of local DB responses. TCP traffic is not considered local traffic for this parameter. Valid values: <ul style="list-style-type: none"> <li>• 0: Disabled</li> <li>• 1: Enabled</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|     |                                   | debug_snapshot                        | 0               | Advanced. Collects a debug dump from a STAP. Should be triggered from the GUI (S-TAP Control > S-TAP commands). After triggering a dump from the GUI, the parameter reverts to its default of 0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|     |                                   | debug_snapshot_level                  | 1               | Advanced. The value of tap_debug_output_level that is run for the debug dump. Valid values: <ul style="list-style-type: none"> <li>• 1: Basic debug</li> <li>• 4: Verbose debug</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|     |                                   | debug_snapshot_time                   | 60              | Advanced. The time interval, in seconds, for which the diagnostic runs. The value can be any integer value.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| GUI                                           | GIM                              | guard_tap.ini               | Default value | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------|----------------------------------|-----------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restricted logging                            |                                  | force_log_limited           | 0             | <p>Controls restricted logging on the collector. Use this to evaluate the number of records affected by an SQL command, while masking the actual query. This parameter can only be set by user root on the DB server. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Unrestricted.</li> <li>• 1: Log with masking. Only logins are allowed (sent packets are flagged with LOGALWAYSMASK). Forces encryption to be on in the S-TAP regardless of any other settings; traffic is sent to the collector only after the collector has indicated that it is aware of the parameter value. Otherwise, the S-TAP logs a message that traffic can't be sent, and its status is red in the S-TAP Control page.</li> <li>• 2: All packets are allowed (sent packets are flagged with LOGACCESSONLY)</li> </ul> |
|                                               | STAP_UID_CHAIN_TRAC              | hunter_trace                | 0             | <p>Turns on the collection of UID chains. When enabled, captures the UID but without IP in the string. Use this setting for local TCP/IP connections including Solaris zones and AIX WPARs, and remote TCP/IP connections when appserver_installed = 1. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Disabled</li> <li>• 1: Enabled</li> </ul> <p>See more information in <a href="#">Linux-UNIX: UID chains</a>. Can be set when pushing to a group of DB servers via GIM.</p>                                                                                                                                                                                                                                                                                                                    |
| Load Balancer IP                              | STAP_LOAD_BALANCER_IP            | load_balancer_ip            |               | Required for enterprise load balancing. If blank, enterprise load balancing is disabled. The IP address or hostname of the central manager or managed unit this S-TAP uses for load balancing.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Managed Units                                 | STAP_LOAD_BALANCER_NUM_MUS       | load_balancer_num_mus       | 1             | The number of managed units the enterprise load balancer allocates for this S-TAP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Load balancer node affinity                   | STAP_LOAD_BALANCER_NODE_AFFINITY | load_balancer_node_affinity |               | <p>Whether the S-TAP connects to more than one managed unit, for enterprise load balancing. Some scenarios need all traffic to go to the same collector. With Oracle ATAP, for example, the analyzed client IP only shows if both the encrypted and unencrypted sessions go to the same managed unit. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Disabled. The S-TAP traffic goes to, at a maximum, the number of managed units specified by load_balancer_num_mus.</li> <li>• 1: Enabled. The S-TAP traffic goes to one managed unit, and has, at a maximum, the number of connections (to that managed unit) specified by load_balancer_num_mus.</li> </ul> <p>See <a href="#">load_balancer_num_mus</a></p>                                                                                   |
|                                               |                                  | merge_with_template         | 0             | <p>Specifies whether the configuration from the collector is merged with the template config file when it is pushed to S-TAP. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Disabled (comments in guard_tap.ini are lost).</li> <li>• 1: Enabled (comments in guard_tap.ini are preserved).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                                               | STAP_SHMID_BLACKLIST             | shmid_blacklist             | NULL          | Comma separated list of shared memory IDs, each one related to a particular process (owner) that the K-TAP filters.<br>Can only be set per Guardium system when updating using GIM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                                               | STAP_SHMID_BLACKLIST_WAIT        | shmid_blacklist_wait        | 0             | <p>Wait to activate interception until shmid_blacklist items are discovered. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Disabled</li> <li>• 1: Enabled</li> </ul> <p>Can be set when pushing to a group of DB servers via GIM.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                                               | STAP_BLACKLIST_SHMEM_OPS_BY_PROC | blacklist_shmem_ops_by_proc | NULL          | K-TAP filters the the shmem interception by this comma separated list of processes.<br>Can only be set per Guardium system when updating using GIM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                                               | STAP_FAM_ENABLED                 | fam_enable                  | 0             | <p>Global enable/disable for FAM. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Disabled</li> <li>• 1: Enabled</li> </ul> <p>FAM rules must be defined in order for FAM to run. If rules are not defined, enabling this parameter opens a connection to the Guardium system on port 16022 (or 16023 if using encryption), but FAM remains essentially disabled.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                                               | STAP_FAM_INSTALLED               | fam_installed               | 0             | <p>Valid values: 0 and 1.<br/>0: FAM module will not be installed.<br/>1: FAM module will be installed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Include client IP in UID chain for SSH daemon | STAP_UID_CHAIN_SSHD_IP           | uid_chain_sshd_ip           | 0             | <p>Add an SSH client IP:port pair to the UID chain when SSH is identified as one of the processes in the chain. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Disabled</li> <li>• 1: Enabled</li> </ul> <p>See more information in <a href="#">Linux-UNIX: UID chains</a>. Can be set when pushing to a group of DB servers via GIM.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| GUI                       | GIM                            | guard_tap.ini             | Default value | Description                                                                                                                                                                                                                                                                                                                                        |
|---------------------------|--------------------------------|---------------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cassandra audit           | STAP_CASSANDRA_AUDIT_ENABLED   | cassandra_audit_enabled   | 0             | <p>Create file appender pipe for Cassandra/Datastax with native audit logging. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Disabled</li> <li>• 1: Enabled</li> </ul> <p>Can be set when pushing to a group of DB servers via GIM.</p>                                                                                            |
| Cassandra audit delimiter | STAP_CASSANDRA_AUDIT_DELIMITER | cassandra_audit_delimiter | GUARD_DELIM   | <p>Cassandra audit reader delimiter. Valid values:</p> <ul style="list-style-type: none"> <li>• Printable ASCII characters a-z A-Z 0-9 - _ ! @ # \$ % ^ &amp; * ()</li> </ul> <p>Can be set when pushing to a group of DB servers via GIM.</p>                                                                                                     |
|                           |                                | exit_lib_num_threads      |               | Hidden parameter. The number of shared memory segments created by the S-TAP. The number of requests for shared memory segments (from the exit library) is equal to the number of instances on the database. The value of this parameter should be equal to or greater than the number of database instances. The default is 10, the maximum is 20. |

## Related concepts

- [Linux-UNIX: Multi-threading S-TAP to increase S-TAP throughput](#)
- [Linux-UNIX: S-TAP load-balancing models and configuration guidelines](#)

## Linux-UNIX: Inspection engine parameters

These parameters affect the behavior of the inspection engine that the S-TAP uses to monitor a data repository on a DB server.

These parameters are stored in the individual [DB\_<name>] inspection engine section of the S-TAP properties file, guard\_tap.ini, with the name of a data repository. There can be multiple sections in a properties file, each describing one inspection engine used by this S-TAP.

| GUI                       | guard_tap.ini    | Default value       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------|------------------|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protocol                  | db_type          |                     | Required. The type of data repository that is monitored.<br>ASTERDB, Cassandra, CockroachDB, CouchDB, DB2®, Db2 Exit, ElasticSearch, exclude IE, FTP, GreenplumDB, HADOOP, HIVE, HP-Vertica, HTTP, HUE, IMPALA, Informix®, Informix Exit, KERBEROS, MariaDB, MemSQL, MongoDB, Mysql, Netezza®, Oracle, PostgreSQL, REDIS, SAP Hana, Sybase, Teradata, Teradata Exit, WebHDFS, Windows File Share                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Port range                | port_range_start |                     | For monitoring network traffic only, the lowest numbered port on which to listen for database traffic. Together with port_range_end, this parameter defines the range of ports that are monitored for this database instance. Usually the range contains only a single port. For a Kerberos inspection engine, set the start and end values to 88-88. If a range is used, do not include extra ports in the range. Extra ports might result in excessive resource consumption while the S-TAP attempts to analyze unwanted traffic.<br>Examples:<br>To monitor range 1521-1525 (five ports) with no port forwarding: <ul style="list-style-type: none"> <li>• port_range_start=1521</li> <li>• port_range_end=1525</li> <li>• real_db_port=1521</li> </ul> To monitor range 2000-2004 (five ports) where network port 2000 is mapped to local port 1521: <ul style="list-style-type: none"> <li>• port_range_start=2000</li> <li>• port_range_end=2004</li> <li>• real_db_port=1521</li> </ul> |
| Port range                | port_range_end   |                     | For monitoring network traffic only, the highest numbered port on which to listen for database traffic.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| KTAP DB Real Port         | real_db_port     | 4100                | With K-TAP and PCAP, identifies the database port or range of ports to be monitored. For exit libraries, use its value for db_home.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Client Ip/Mask            | networks         | 0.0.0.0/0.0.0.0::/0 | Restricts S-TAP to monitor traffic only from the specified sets of IP address and mask pairs, by using a list of addresses in IP address/mask format: n.n.n.n/m.m.m.m. If an improper IP address/mask is entered, the S-TAP does not start. Valid values: <ul style="list-style-type: none"> <li>• User-defined list</li> <li>• 0.0.0.0/0.0.0.0::/0: select all clients.</li> <li>• 127.0.0.1/255.255.255.255::1/0: local traffic only</li> </ul> Client Ip/Mask (networks) and Exclude Client Ip/Mask (exclude networks) cannot be specified simultaneously. If the value of this parameter is not configured correctly, the value is replaced by the default value.                                                                                                                                                                                                                                                                                                                          |
| Exclude Client Ip/Mask    | exclude_networks |                     | A list of client IP addresses and corresponding masks that are excluded from monitoring. Use this option to configure the S-TAP to monitor all clients, except for a certain client or subnet (or a collection thereof). Client Ip/Mask (networks) and Exclude Client Ip/Mask (exclude networks) cannot be specified simultaneously.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| TEE Listen Port-Real Port | tee_listen_port  |                     | Deprecated. Replaced by the parameter real_db_port when the K-TAP monitoring mechanism is used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Connect To Ip             | connect_to_ip    | 127.0.0.1::1        | IP address for S-TAP to use to connect to the database. Some databases accept local connection only on the real IP address of the Guardium® system, and not on the default (127.0.0.1::1). When K-TAP is enabled, this parameter is used for Solaris zones and AIX® WPARs. Set it to the zone IP address to capture traffic.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| GUI                | guard_tap.ini             | Default value | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|---------------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DB User            | db_user                   | NULL          | OS username (case-sensitive) of the owner of the DB server process (for example, oracle). This parameter specifies which user is allowed to use the db_request_handler socket. It is required if you are not using the user root. If set to an invalid value, A-TAP cannot access the socket to retrieve permission for accessing K-TAP. In this case, it requires authorization with a group membership to log decrypted traffic to K-TAP (by using the <b>guardctl authorize-user</b> command). You can define a comma-separated string of multiple users.                                                                                                                                                                                                                                                                                               |
| DB Install Dir     | db_install_dir            | NULL          | <ul style="list-style-type: none"> <li>Db2®, Informix: The full path name for the database installation directory.</li> <li>Db2 exit and Informix exit: value must be the same as the \$HOME value in the database (or \$Db2_HOME for Db2 Exit); otherwise tap_identifier does not function properly.</li> <li>Oracle: Database owner HOME directory. It must match db_base in the ATAP configuration. See <a href="#">Linux-UNIX: Oracle-specific guardctl parameters</a>.</li> <li>All other database types: NULL.</li> </ul>                                                                                                                                                                                                                                                                                                                            |
| Process Name       | db_exec_file              | NULL          | <p>The value of this parameter depends on whether it's in an exit, and whether there is A-TAP.</p> <ul style="list-style-type: none"> <li>Exit libraries: see <a href="#">Linux-UNIX: Configuring Exit libraries</a></li> <li>With A-TAP: see <a href="#">Linux-UNIX: Database-specific guardctl parameters</a></li> <li>Without A-TAP: The full path name for the database executable. For example: <ul style="list-style-type: none"> <li>Oracle: /\$ORACLE_HOME/bin/oracle</li> <li>Informix: /INFORMIXTMP/.inf.sqlexec. Applies to all Informix platforms but Linux®.</li> <li>Informix with Linux, example: /home/informix11/bin/oninit</li> <li>MySQL: mysql</li> </ul> </li> </ul>                                                                                                                                                                  |
| Encryption         | encryption                | 0             | <p>Valid values:</p> <ul style="list-style-type: none"> <li>0: Unencrypted</li> <li>1: Encrypted</li> </ul> <p>Default = 0 (false)</p> <p>Activate ASO or SSL encrypted traffic for Oracle (versions 11 and 12) and Sybase on Solaris, HPUX, and AIX.</p> <p>For Oracle, specify db_version in the guard_tap.ini file (for example, db_version=12)</p> <p>For Oracle12 SSL, instrument on all platforms. For Oracle11 SSL, instrument on AIX.</p> <p>For any Oracle requiring instrumentation, if you are using encryption=1 in the guard_tap.ini (which is not supported on Linux), you must instrument before setting that parameter.</p> <p>Some DBs require restart after enabling encryption.</p> <p>When using GIM to configure the S-TAP, GIM_ROOT_DIR must be set to the absolute path to the modules, for example /usr/local/guardium/modules</p> |
|                    | load_balanced             | 1             | <p>Valid values:</p> <ul style="list-style-type: none"> <li>0: Database traffic does not participate in load balancing.</li> <li>1: Database traffic participates in load balancing.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                    | priority_count            | 20            | <p>Reduces the instances of a blank DB_USER or ? in the tables. At session creation, the first priority_count packets are marked with a high priority flag and are transferred to a special high priority queue on the collector. Valid values:</p> <ul style="list-style-type: none"> <li>0: Disabled</li> <li>Protocol 7: 1-2048: Number of packets</li> <li>Protocol 8: positive integer: Number of packets</li> </ul> <p>Default = 20</p>                                                                                                                                                                                                                                                                                                                                                                                                              |
| Intercept Types    | intercept_types           | NULL          | <p>DO NOT change this parameter unless it is absolutely necessary. Protocol types that are intercepted by the IE.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>NULL: auto intercepts all protocols the Database supports</li> <li>Comma-separated list: IE intercepts these protocol types only.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Identifier         | tap_identifier            | NULL          | Used to distinguish inspection engines from one another. If unspecified, Guardium auto-populates the field with a unique name that uses the database type and sequence number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| DB Version         | db_version                | 9             | The database version. The string must start with a numeral and not a letter.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Unix Socket Marker | unix_domain_socket_marker | Null          | Specifies UNIX domain sockets marker for Oracle, MySQL, and Postgres. Usually the default is correct, but when the named pipe or UNIX domain socket traffic does not work then you need to make sure that this value is set correctly. For example, for Oracle, set unix_domain_socket_marker to the KEY of IPC defined in tnsnames.ora. If it is NULL or not set, the S-TAP uses defined default markers identified as: * MySQL - "mysql.sock" * Oracle - "./oracle/" * Postgres - ".s.PGSQL.5432"                                                                                                                                                                                                                                                                                                                                                        |

## Parameters used with IBM Db2 databases

The script **find\_db2\_shmem\_parameters.sh**, located in `stap_directory/bin`, outputs what the Db2 shared memory parameters defined in the Inspection Engines should be. Execute it either as root or Db2 user, using the syntax: **find\_db2\_shmem\_parameters.sh <instance name>**. You can run it from any directory.

Table 1. Additional S-TAP configuration parameters for a Db2 inspection engine

| GUI                     | guard_tap.ini           | Default value | Description                                                                                                                                                                                                                                                                                      |
|-------------------------|-------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DB2 Shared Mem. Adjust. | db2_fix_pack_adjustment | 20            | Required when Db2 is selected as the database type, and shared memory connections are monitored. The offset to the server's portion of the shared memory area. Offset to the beginning of the Db2 shared memory packet, depends on the Db2 version: 32 in pre-8.2.1, and 80 in 8.2.1 and higher. |

| GUI                      | guard_tap.ini             | Default value | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------|---------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DB2 Sh. Mem. Client Pos. | db2_shmem_client_position | 61440         | The offset to the client's portion of the shared memory area. Required when Db2 is selected as the database type, and shared memory connections are monitored. Use the script find_db2_shmem_parameters.sh to find the value. The script is located in <code>stap_directory/bin</code> , and outputs what the Db2 shared memory parameters that are defined in the Inspection Engines should be. Run it either as root or Db2 user, by using the syntax: <code>find_db2_shmem_parameters.sh &lt;instance name&gt;</code> . You can run it from any directory. |
|                          | db2bp_path                | Null          | Relevant only when using A-TAP on Db2. If the program 'db2bp' (part of Db2) is in the standard location, db2bp_path does not need to be set. If it is non-standard, then this parameter points to its location. Set this parameter to the full path of the relevant db2bp as seen from the global zone or WPAR. For example, if the file is /data/db2inst1/sqllib/bin/db2bp and the zone is installed in /data/zones/oracle2nd/root/ then set the full path (db2bp_path) as /data/zones/oracle2nd/root/data/db2inst1/sqllib/bin/db2bp                         |
| DB2 Shared Mem. Size     | db2_shmem_size            | 131072        | Db2 shared memory segment size. Required when Db2 is selected as the database type, and shared memory connections are monitored.                                                                                                                                                                                                                                                                                                                                                                                                                              |

## Linux-UNIX: Oracle Unified Auditing parameters

These parameters define the Oracle Unified Auditing connection between the S-TAP and the SQL server.

These parameters are stored in the individual [SQLC\_<integer>] sections of the S-TAP properties file, guard\_tap.ini. There can be multiple sections in a properties file, each describing one connection for pulling data from a database, which is used by this S-TAP.

Note: The password can be defined only with the API command [store\\_sql\\_credentials](#).

| GUI                       | guard_tap.ini      | Default value | Description                                                                                                                                                                                                                                                                                                                        |
|---------------------------|--------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DB type                   | db_type            |               | Required. The type of data monitored repository. Valid value: <ul style="list-style-type: none"><li>• Oracle</li></ul>                                                                                                                                                                                                             |
| Instance name             | instance           |               | Required. service_name that specifies the connection identifier in the tnsnames.ora that is used to connect to the database.                                                                                                                                                                                                       |
| Data pull interval (sec.) | data_pull_interval | 30            | Frequency, in seconds, of S-TAP polls of the audit table that looks for new data.                                                                                                                                                                                                                                                  |
| User name                 | username           |               | Required. User name of a user with access to the database and permission to read entries in the unified audit table.                                                                                                                                                                                                               |
| User role                 | role               |               | Role for user with access to the database and permission to read entries in the audit table, for example, for a user name "sys", you might specify a user role of "sysdba"                                                                                                                                                         |
| Data pull number of rows  | data_pull_rows     | 100           | The number of rows to attempt to pull in one iteration. Each check interval, S-TAP attempts to pull the full amount of new data to the collector. Use this parameter to tune the amount of memory that is used by the S-TAP versus impact on the database for collecting data. It is recommended to leave it at the default value. |
| Timeout (sec.)            | timeout            | 300000        | Time, in seconds, to allow the database to respond.                                                                                                                                                                                                                                                                                |

## Related tasks

- [Linux-UNIX: Configuring S-TAP interception using Oracle Unified Audit](#)

## Related information

- [Oracle Unified Audit Activity](#)
- [Oracle Unified Audit \(S-TAP Configuration\) Activity](#)

## Linux-UNIX: Firewall parameters

These parameters affect the behavior of the S-TAP with respect to the firewall.

These parameters are stored in the [TAP] section of the S-TAP properties file.

| GUI                | GIM                     | guard_tap.ini      | Default value | Description                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|-------------------------|--------------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Firewall installed | STAP_FIREWALL_INSTALLED | firewall_installed | 0             | Firewall feature enabled. Valid values: <ul style="list-style-type: none"><li>• 0: Disabled.</li><li>• 1: Enabled.</li></ul><br>Note: firewall_installed and qrw_installed cannot be enabled at the same time. If qrw_installed is set to 1, then firewall_installed is disabled.                                                                                     |
| Firewall timeout   | STAP_FIREWALL_TIMEOUT   | firewall_timeout   | 2             | Time to wait for a verdict from the Guardium® system. If the firewall times out, the value of the parameter firewall_fail_close determines whether to block or allow the connection.<br>Valid values: -1 to -999, 1 to 10.<br>Negative values represent milliseconds and positive values represent seconds. For example, -50 is 50 milliseconds while 3 is 3 seconds. |

| GUI                    | GIM                         | guard_tap.ini          | Default value | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------|-----------------------------|------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Firewall fail close    | STAP_FIREWALL_FAIL_CLOSE    | firewall_fail_close    | 0             | The action when the verdict cannot be set by the policy rules, for example the Firewall timeout expires. Valid values: <ul style="list-style-type: none"><li>• 0: the connection goes through.</li><li>• 1: the connection is blocked.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Firewall default state | STAP_FIREWALL_DEFAULT_STATE | firewall_default_state | 0             | Sets the firewall activation trigger. Must be 0 if <a href="#">qrw_default_state=1</a> or 2. Valid values: Valid values: <ul style="list-style-type: none"><li>• 0: Firewall is activated per session when triggered by a rule in the installed policy.</li><li>• 1: All traffic is watched for firewall policy violations</li><li>• 2: All traffic is watched for firewall policy violations for the initial priority_count packets (guard_tap.ini parameter). S-TAP watches the initial part of every new session to your DB. This is useful when you have session based policies, firewall rules based on the user, or some other information that is passed early in the session. It limits the impact of firewall on the performance. Instead of watching every bit of the session (Firewall default state=1) and waiting for an UNWATCH verdict, S-TAP simply unwatches automatically if no WATCH or DROP is sent.<br/>To reduce the possibility that short sessions evade firewall and redaction rules, if either firewall_default_state or qrw_default_state is set to 2, create a session-level policy. S-TAP watches all priority packets and sends them to collector, which reduces the chance of avoiding firewall or redaction rules.</li></ul> |
| Firewall force watch   | STAP_FIREWALL_FORCE_WATCH   | firewall_force_watch   | NULL          | When firewall_default_state=0 (off), then firewall_force_watch specifies the network/mask of the IPs you want the firewall to watch, overriding the default (off).<br>Valid value: comma separated list of IP/mask values.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Firewall force unwatch | STAP_FIREWALL_FORCE_UNWATCH | firewall_force_unwatch | NULL          | When firewall_default_state=1 (on), then firewall_force_unwatch specifies the network/mask of the IPs you want the firewall to ignore, overriding the default (on).<br>Valid value: comma separated list of IP/mask values.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Linux-UNIX: Query rewrite parameters

The query rewrite parameters affect the behavior of the S-TAP with respect to discovery.

| GIM                    | guard_tap.ini     | Default Value | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------|-------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| STAP_QRW_INSTALLED     | qrw_installed     | 0             | Enable or disable the query rewrite feature. When set to 0, all other parameters in this group are ignored. Valid values: <ul style="list-style-type: none"><li>• 0: Disabled</li><li>• 1: Enabled</li></ul><br>Note: firewall_installed and qrw_installed cannot be enabled at the same time. If qrw_installed is set to 1, then firewall_installed is disabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| STAP_QRW_DEFAULT_STATE | qrw_default_state | 0             | Sets the query rewrite activation trigger. Must be 0 if <a href="#">firewall_default_state=1</a> or 2. Valid values: <ul style="list-style-type: none"><li>• 0: QRW is activated per session when triggered by a rule in the installed policy.</li><li>• 1: Watch all packets. QRW is activated for every session regardless of the installed policy. S-TAP watches all priority packets and sends them to collector, which reduces the chance of avoiding firewall or redaction rules.</li><li>• 2: Priority packets are watched by default. If event is not triggered by the priority packets, then query rewrite stops watching after priority packets until the policy is triggered. To reduce the possibility that short sessions evade firewall and redaction rules, when either qrw_default_state or firewall_default_state is set to 2, create a session-level policy. Firewall/QRW is initially activated for a limited number of the first packets (priority packets) of each session. If not triggered by the rule of the installed SLP policy, then Firewall/QRW is automatically deactivated.<br/>When set to 2, the QRW operation can be modified by the following commands:<ul style="list-style-type: none"><li>◦ <b>Watch</b> - S-TAP changes the state from 2 to 1 so that the connection is permanently subject to firewall or query rewrite operations.</li><li>◦ <b>Drop</b> - Terminate the connection immediately.</li><li>◦ <b>Watch &amp; Drop</b> - Terminate the connection immediately.</li><li>◦ <b>Unwatch</b> - S-TAP changes the state from 2 to 0 so the connection is no longer subject to firewall or query rewrite operations.</li></ul></li></ul> |
| STAP_QRW_FORCE_WATCH   | qrw_force_watch   | NULL          | Comma-separated list of client IP/MASKs (for example, 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2) to watch automatically. Valid when qrw_installed is 1, and qrw_default_state is 0. Cannot be configured to the same IP range as firewall_force_unwatch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| STAP_QRW_FORCE_UNWATCH | qrw_force_unwatch | NULL          | Comma separated list of client IP/MASKs (for example, 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2) to exclude from watching. Valid when qrw_installed is 1, and qrw_default_state is 1. Cannot be configured to the same IP range as firewall_force_watch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Linux-UNIX: Server-side masking (SSM) parameters

The server-side masking parameters affect the behavior of the S-TAP with respect to discovery.

These parameters are stored in the [TAP] section of the S-TAP properties file.

Attention: These are advanced parameters and should be modified only by IBM Technical Support.

| Parameter                         | Default value | Description                                                                                                                                                                                                                                                                  |
|-----------------------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| server_side_masking_installed     | 0             | Enables the server-side masking feature. Valid values: <ul style="list-style-type: none"><li>• 0=No</li><li>• 1=Yes</li></ul>                                                                                                                                                |
| server_side_masking_default_state | 0             | Sets the server-side masking activation trigger. Valid values: <ul style="list-style-type: none"><li>• 0=SSM activated per session when triggered by a rule in the installed policy</li><li>• 1=SSM activated for every session regardless of the installed policy</li></ul> |
| server_side_masking_force_watch   | NULL          | Comma separated list of client IP/MASKs (for example, 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2) whose sessions are watched automatically. Valid when server_side_masking_installed=1 and qrw_default_state=0. Cannot be configured to the same range as firewall_force_watch.         |
| server_side_masking_force_unwatch | NULL          | Comma separated list of client IP/MASKs (for example, 1.1.1.1/1.1.1.1,2.2.2.2/2.2.2.2) whose sessions are not watched. Valid when server_side_masking_installed is 1 and firewall_default_state is 1. Cannot be configured to the same range as firewall_force_unwatch.      |

## Linux-UNIX: Discovery parameters

The discovery parameters define the behavior of the auto-discovery feature, for discovering database instances and sending the results to the current active S-TAP.

Attention: These are advanced parameters and should be modified only by IBM Technical Support.

| GIM                                | guard_tap.ini                 | Default value                                                             | Description                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------|-------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| STAP_DISCOVERY_INTERVAL            | discovery_interval            | 24                                                                        | The time interval at which auto-discovery runs. Valid values: <ul style="list-style-type: none"><li>• 0: disabled</li><li>• &lt; 0: interval in minutes</li><li>• &gt; 0: interval in hours</li></ul> Default = 24 (hours)                                                                                                                                  |
| STAP_DISCOVERY_DBs                 | discovery_dbs                 | oracle:db2:informix:mysql:pos:tgres:sybase:hadoop:teradata:netezza:memsql | Colon (':') separated list of database types to attempt to discover. Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                                                              |
| STAP_DISCOVERY_DEBUG               | discovery_debug               | 0                                                                         | Output debug information from discovery. The log is guard_discovery.stderr.log located in the directory specified by the parameter tap_log_dir (by default: /tmp/guard_stap). <ul style="list-style-type: none"><li>• 0: disable (errors only)</li><li>• 1: errors and debug statements</li></ul> Can be set when pushing to a group of DB servers via GIM. |
| STAP_DISCOVERY_ORA_ALT_LOCATIONS   | discovery_ora_alt_locations   |                                                                           | Alternate locations to look for listener.ora files. Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                                                                               |
| STAP_DISCOVERY_ORA_USE_PORT_RANGES | discovery_ora_use_port_ranges | 0                                                                         | Enable S-TAP discovery of Oracle databases to combine discovered instances based on port ranges. This setting works with a single unix_domain_socket_marker. Multiple unix_domain_socket_marker configurations require separate instances. Valid values: <ul style="list-style-type: none"><li>• 0: disabled</li><li>• 1: enabled</li></ul>                 |
| STAP_DISCOVERY_PORT                | discovery_port                | 8443                                                                      | S-TAP Discovery uses this port to connect to the Guardium® system.                                                                                                                                                                                                                                                                                          |

## Linux-UNIX: Application server parameters

These parameters affect the behavior of the S-TAP when an application user name needs to be bounded with database activities.

These parameters are in the [TAP] section on the guard\_tap.ini file.

For more information, see [Linux-UNIX: Application server S-TAP configuration](#).

| GUI                             | GIM                          | guard_tap.ini           | Default value | Description                                                                                                                                                              |
|---------------------------------|------------------------------|-------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| App. Server User Identification | STAP_APPSERVER_INSTALLED     | appserver_installed     | 0             |                                                                                                                                                                          |
| Ports                           | STAP_APPSERVER_PORTS         | appserver_ports         | 8080          | Comma-separated list of ports, or hyphens for inclusive ranges of ports, on which the Java™ application is accessed by a web browser.                                    |
| Login pattern                   | STAP_APPSERVER_LOGIN_PATTERN | appserver_login_pattern |               | Comma-separated list of strings specifying the login pattern that is passed to the application. This pattern is passed to the Java application to identify a user login. |

| GUI                | GIM                             | guard_tap.ini              | Default value | Description                                                                                                                                                                                                                        |
|--------------------|---------------------------------|----------------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Username prefix    | STAP_APPSERVER_USERNAME_PREFIX  | appserver_username_prefix  |               | Comma-separated list of strings specifying the prefix to the username for a specific session. This is the pattern the Java application uses to indicate the username of the given session.                                         |
| Username postfix   | STAP_APPSERVER_USERNAME_POSTFIX | appserver_username_postfix |               | Comma-separated list of strings specifying the postfix to the username for a specific session. This pattern is passed to the Java application to indicate the end of the value for the given variable that indicates the username. |
| Session pattern    | STAP_APPSERVER_SESSION_PATTERN  | appserver_session_pattern  |               | Comma-separated list of strings specifying the start of an end-user session, using a particular database session. This pattern specifies the [change of] end-user session for a specific database connection.                      |
| Session prefix     | STAP_APPSERVER_SESSION_PREFIX   | appserver_session_prefix   |               | Comma-separated list of strings specifying the session identifier.                                                                                                                                                                 |
| Session postfix    | STAP_APPSERVER_SESSION_POSTFIX  | appserver_session_postfix  |               | Comma-separated list of strings specifying where the session ends.                                                                                                                                                                 |
| Session ID pattern | STAP_APPSERVER_USERSESS_PATTERN | appserver_usersess_pattern |               | Comma-separated list of strings specifying the identifier for marking which end-user session a specific connection is continuing with.                                                                                             |
| Session ID prefix  | STAP_APPSERVER_USERSESS_PREFIX  | appserver_usersess_prefix  |               | Comma-separated list of strings specifying what identifies or precedes the session_id in a specific users indicator packet.                                                                                                        |
| Session ID postfix | STAP_APPSERVER_USERSESS_POSTFIX | appserver_usersess_postfix |               | Comma-separated list of strings specifying where the session ID ends.                                                                                                                                                              |

## Linux-UNIX: Hadoop parameters

Guardium supports Hadoop integration using HDFS, Hortonworks with Apache Ranger, and Cloudera Navigator. Understand the S-TAP configuration required for these integrations.

- [Parameters for HDFS](#)
- [Parameters for Hortonworks with Apache Ranger](#)
- [Parameters for Cloudera Navigator using Kafka messaging](#)

### Parameters for HDFS

Table 1. Parameters for HDFS integration

| GUI                              | GIM                                   | guard_tap.ini                    | Default | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------|---------------------------------------|----------------------------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ranger HDFS audit directories    | STAP_RANGER_HDFS_AUDIT_DIRS           | ranger_hdfs_audit_dirs           | NULL    | Comma-separated list of directories where Ranger logs the service audits. Include one directory that contains the daily log directories, for each service you want to monitor. Usually the paths are located under /ranger/audit.<br><br>Example service directories for CDP 7:<br>/ranger/audit/hive/hiveServer2,/ranger/audit/kafka/kafka,/ranger/audit/hbase/hbaseMaster,/ranger/audit/hbase/hbaseRegional,/ranger/audit/atlas/atlas,/ranger/audit/hdfs/hdfs<br><br>Example service directories for HW 3:<br>/ranger/audit/hbaseMaster,/ranger/audit/hbaseRegional,/ranger/audit/hdfs,/ranger/audit/hiveServer2,/ranger/audit/kafka,/ranger/audit/solr,/ranger/audit/storm |
| Ranger HDFS audit history length | STAP_RANGER_HDFS_AUDIT_HISTORY_LENGTH | ranger_hdfs_audit_history_length | 30      | The length of the audit history. <ul style="list-style-type: none"> <li>A value of 0 means that the S-TAP will read audits from the beginning of time.</li> <li>A positive value (max = 2147483647) is the history length in days. The default is 30 days.</li> <li>A negative value (min = -2147483648) is the history length in hours.</li> </ul>                                                                                                                                                                                                                                                                                                                           |
| Ranger HDFS keytab               | STAP_RANGER_HDFS_KEYTAB               | ranger_hdfs_keytab               | NULL    | Required for Kerberos. Location of the Kerberos keytab that contains the principal used to connect to HDFS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Ranger HDFS lib location         | STAP_RANGER_HDFS_LIB_LOCATION         | ranger_hdfs_lib_location         | NULL    | Locate libhdfs.so provided by Hadoop cluster (for example, /usr/hdp/3.1.0.141-1/usr/lib/libhdfs.so) and set ranger_hdfs_lib_location to the directory that contains libhdfs.so (for example, /usr/hdp/3.1.0.141-1/usr/lib).                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| HDFS name node                   | STAP_RANGER_HDFS_NAMENODE             | ranger_hdfs_namenode             | NULL    | IP or hostname of the HDFS NameNode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Ranger HDFS poll (milliseconds)  | STAP_RANGER_HDFS_POLL_MS              | ranger_hdfs_poll_ms              | 100     | Time interval, in milliseconds, the S-TAP waits between checking for new Ranger audits in HDFS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| HDFS port                        | STAP_RANGER_HDFS_PORT                 | ranger_hdfs_port                 | 8020    | The HDFS NameNode port the S-TAP connects to.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                                  | STAP_RANGER_HDFS_READER_ENABLED       | ranger_hdfs_reader_enabled       | 0       | Whether the Ranger HDFS reader is enabled. Valid values: <ul style="list-style-type: none"> <li>0: Disabled</li> <li>1: Enabled</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| GUI              | GIM                   | guard_tap.ini    | Default | Description                                                                                                                                                                                                                                                                                     |
|------------------|-----------------------|------------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ranger HDFS user | STAP_RANGER_HDFS_USER | ranger_hdfs_use  | NULL    | The user with which S-TAP connects to HDFS. if the HDFS setup is using Kerberos, set the parameter to the Kerberos principal.                                                                                                                                                                   |
| LD library path  | STAP_LD_LIBRARY_PATHS | ld_library_paths | NULL    | Locate libjvm.so (for example, /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.191.b12-1.el7_6.x86_64/jre/lib/amd64/server/libjvm.so) and set ld_library_paths to the directory that contains libjvm.so (for example, /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.191.b12-1.el7_6.x86_64/jre/lib/amd64/server). |

## Parameters for Hortonworks with Apache Ranger

Some parameters are configurable through the Guardium user interface or through the Guardium Installation Manager. All parameters are configurable using the Guardium API.

Attention: These are advanced parameters and should be modified only by IBM Technical Support.

Table 2. Parameters for Hortonworks with Apache Ranger integration

| GIM                                        | guard_tap.ini                         | Default value | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------|---------------------------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| STAP_LOG4J_READER_ENABLED                  | log4j_reader_enabled                  | 0             | Enable log4j listening mode for Ranger traffic. Valid values: <ul style="list-style-type: none"><li>• 0: disabled</li><li>• 1: enabled</li></ul>                                                                                                                                                                                                                                                                                                                 |
| STAP_LOG4J_PORT                            | log4j_port                            | 5555          | The port where the Guardium S-TAP listens for Ranger audits (integer value). Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                                                                                                                                                           |
| STAP_LOG4J_LISTEN_ADDRESS                  | log4j_listen_address                  | 0.0.0.0       | IP Address for log4j listener, for Ranger plug ins. The default value of 0.0.0.0 is recommended, as this enables the S-TAP to receive traffic from any host. Use localhost if configuring the system for high availability (indicates the loopback address of the system). If you choose to restrict access to a specific address, be sure you are not excluding any necessary traffic for monitoring. Can be set when pushing to a group of DB servers via GIM. |
| STAP_LOG4J_NUM_CONNECTIONS                 | log4j_num_connections                 | 20            | The number of concurrent connections (integer) to expect from the service or services defined for this S-TAP. Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                                                                                                                          |
| STAP_RANGER_DYNAMIC_POLICY_PORT            | ranger_dynamic_policy_port            | 5556          | Port that Ranger plugins connect to. S-TAP listens here for the Ranger dynamic policy. Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                                                                                                                                                 |
| STAP_RANGER_DYNAMIC_POLICY_LISTEN_ADDRESS  | ranger_dynamic_policy_listen_address  | 0.0.0.0       | Ranger dynamic policy reader listener port. <ul style="list-style-type: none"><li>• 0.0.0.0 indicates any IP address of the system</li><li>• Use localhost for HA</li></ul> Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                                                            |
| STAP_RANGER_DYNAMIC_POLICY_NUM_CONNECTIONS | ranger_dynamic_policy_num_connections | 20            | Maximum allowed connections for Ranger dynamic policy reader. Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                                                                                                                                                                          |
| STAP_RANGER_DYNAMIC_POLICY_TIMEOUT         | ranger_dynamic_policy_timeout         | 10            | Timeout, in seconds, for Ranger dynamic policy reader policy verdicts. Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                                                                                                                                                                 |
| STAP_RANGER_DYNAMIC_POLICY_DEFAULT_VERDICT | ranger_dynamic_policy_default_verdict | 1             | Default policy verdict for Ranger dynamic policy reader when the verdict times out. Valid values: <ul style="list-style-type: none"><li>• 0: block</li><li>• 1: pass</li></ul> Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                                                         |
| STAP_RANGER_DYNAMIC_POLICYREADER_ENABLED   | ranger_dynamic_policy_reader_enabled  | 0             | Enable Hortonworks dynamic policy reader. Valid values: <ul style="list-style-type: none"><li>• 0: disabled</li><li>• 1: enabled</li></ul> Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                                                                                             |

## Parameters for Cloudera Navigator using Kafka messaging

Guardium supports Cloudera Navigator for collecting audit data using the Kafka messaging system.

Some parameters are configurable through the Guardium user interface or through the Guardium Installation Manager. All parameters are configurable using the Guardium API.

Attention: These are advanced parameters and should be modified only by IBM Technical Support.

Table 3. guard\_tap.ini parameters for Cloudera Navigator using Kafka messaging integration

| GUI | GIM                      | guard_tap.ini        | Default | Description                                                                                                                                                              |
|-----|--------------------------|----------------------|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     | STAP_KAFKAREADER_ENABLED | kafka_reader_enabled | 0       | Enables Cloudera Navigator integration using Kafka publish and consume. Valid values: <ul style="list-style-type: none"><li>• 0: disabled</li><li>• 1: enabled</li></ul> |

| GUI                 | GIM                          | guard_tap.ini           | Default              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------|------------------------------|-------------------------|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bootstrap servers   | STAP_KAFKA_BOOTSTRAP_SERVERS | kafka_bootstrap_servers |                      | Required. The comma separated list of host_name:port pairs is used to establish the initial connection to the Kafka cluster. After the initial connection is established, all servers in the cluster are used. Consider specifying more than one bootstrap in case one is down. Example: hostnameofbroker1:9092,hostnameofbroker2:9092                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Enable TLS          | STAP_KAFKA_USE_TLS           | kafka_use_tls           | 0                    | Whether the Kafka cluster uses TLS. Valid values: <ul style="list-style-type: none"><li>• 0: disabled</li><li>• 1: enabled</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Topic name          | STAP_KAFKA_TOPIC_NAME        | kafka_topic_name        | NavigatorAuditEvents | Required. The topic name in the Kafka cluster that Cloudera publishes audits to, and that S-TAP reads audits from.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Principal           | STAP_KAFKA_PRINCIPAL         | kafka_principal         | NULL                 | The Kerberos principal name for the S-TAP, which is used when the Kafka cluster requires Kerberos authentication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                     | STAP_KAFKA_MESSAGE_MAX_BYTES | kafka_message_max_bytes | 65536                | The maximum number of bytes of messages to attempt to fetch for each topic-partition in each fetch request. The fetch request size must be at least as large as the maximum message size that the Kafka broker(s) that is connected to the S-TAP allows. Otherwise the Cloudera Navigator Audit server that is publishing audits to the Kafka cluster can send messages larger than the S-TAP can fetch. If there is a message larger than the value of this parameter, S-TAP skips that audit and continues.<br>There is no maximum size for this parameter. Best practice is to set it to the same value as the Kafka broker's message.max.bytes. This ensures that the S-TAP can handle the same maximum message size as the broker. Increase the S-TAP buffer size if needed. If you increase kafka_message_max_bytes, the S-TAP allocates more memory, in order to hold the maximum message size. |
| Path to keytab file | STAP_KAFKA_KEYTAB            | kafka_keytab            | NULL                 | The path to the Kerberos keytab file on the S-TAP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Group name          | STAP_KAFKA_GROUP_NAME        | kafka_group_name        | NULL                 | Required. Assigns the S-TAP to this Kafka consumer group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| SSL CA path         | STAP_KAFKA_SSL_CA_LOCATION   | kafka_ssl_ca_location   | NULL                 | Required if kafka_use_tls = 1. Path to the certificate authority (CA) for verifying the Kafka cluster certificate.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| LD library path     | STAP_LD_LIBRARY_PATHS        | ld_library_paths        | NULL                 | Required. A colon delimited list of paths to search for Kafka libraries. Kafka libraries are located in the stap install directory. Set this parameter to the directory containing the guard_stap binary. (Examples: /usr/local/guardium/guard_stap, /usr/local/modules/STAP/current, /opt/guardium/modules/STAP/current.)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Linux-UNIX: Configuration Auditing System (CAS) parameters

These parameters affect the behavior of CAS.

Table 1. CAS parameters for UNIX/Linux

| GUI                       | guard_tap.ini                 | Default value     | Description                                                                 |
|---------------------------|-------------------------------|-------------------|-----------------------------------------------------------------------------|
| Task checkpoint           | cas_task_checkpoint           | task_checkpoint   |                                                                             |
| Client checkpoint         | cas_client_checkpoint         | client_checkpoint |                                                                             |
| Checkpoint period         | cas_checkpoint_period         | 60                |                                                                             |
| Fail over file            | cas_fail_over_file            | fail_over_file    |                                                                             |
| Fail over file size limit | cas_fail_over_file_size_limit | 50000             |                                                                             |
| Max rec. attempts         | cas_max_reconnect_attempts    | 5000              |                                                                             |
| Reconnect interval        | cas_reconnect_interval        | 60                |                                                                             |
| Raw data limit            | cas_raw_data_limit            | 1000              |                                                                             |
| Md5 data limit            | cas_md5_size_limit            | 1000              |                                                                             |
|                           | cas_command_wait              | 300               | Wait time in seconds before killing a long-running data collection process. |
|                           | cas_server_failover_delay     | 60                | Wait time in minutes before trying to connect to another Guardium system.   |

Table 2.

Deprecated  
guardtap.ini  
parameters

|                     |
|---------------------|
| cas_task_baseline   |
| cas_client_baseline |

## Linux-UNIX: Debug parameters

These parameters affect the behavior of S-TAP debugging.

Attention: These are advanced parameters and should be modified only by IBM Technical Support.

These parameters are in the [TAP] section on the guard\_tap.ini file.

Table 1. S-TAP configuration parameters for debugging

| GUI | GIM | guard_tap.ini | Default value | Description |
|-----|-----|---------------|---------------|-------------|
|-----|-----|---------------|---------------|-------------|

| GUI             | GIM                  | guard_tap.ini          | Default value | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------|----------------------|------------------------|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Messages Syslog | STAP_SYSLOG_MESSAGES | syslog_messages        | 1             | <p>Send messages to syslog. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: do not send messages</li> <li>• 1: send messages to syslog</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                |
|                 |                      | tap_debug_output_level | 0             | <p>S-TAP logs level. Logs are stderr.txt, guard_stap.fam.txt located in the directory specified in tap_log_dir parameter (by default: /tmp/guard_stap). Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Disable</li> <li>• 1: Basic debug</li> <li>• 4: Verbose debug</li> <li>• 6: Appserver debug</li> <li>• 10: Exit engine debug. Debug information is logged in both S-TAP log and db2_exit log (db2diag.log).</li> <li>• 11: exit engine debug. Debug information is only logged in db2_exit log (db2diag.log).</li> </ul> |
| Messages Remote | STAP_REMOTE_MESSAGES | remote_messages        | 1             | <p>Send messages to the active Guardium host. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: Do not send messages</li> <li>• 1: Send messages to the active Guardium system.</li> </ul>                                                                                                                                                                                                                                                                                                                                         |

## Linux-UNIX: K-TAP parameters

These parameters affect the behavior of the K-TAP.

These parameters are located in the [TAP] section of the S-TAP properties file: guard\_tap.ini.

Attention: These are advanced parameters and should be modified only by IBM Technical Support.

Table 1. K-TAP configuration parameters

| GIM                         | guard_tap.ini          | Default value | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------|------------------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                             | ktap_installed         | 1             | <p>Whether or not the Kernel Monitor module is installed. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: no</li> <li>• 1: yes</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                               |
| STAP_KTAP_REQUEST_TIMEOUT   | ktap_request_timeout   | 5             | <p>Maximum amount of time, in seconds, to wait for a non-firewall verdict from S-TAP. It can have any value. Can be set when pushing to a group of DB servers via GIM.</p>                                                                                                                                                                                                                                                                                                                                                                                            |
|                             | ktap_dbgev_ev_list     | 0             | <p>It is used to enable K-TAP trace log either through GUI or through guard_tap.ini file. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: disable</li> <li>• 1: enable ktap trace log located under /var/tmp directory</li> </ul>                                                                                                                                                                                                                                                                                                                       |
|                             | ktap_dbgev_func_name   | all           | <p>List of functions to log in K-TAP trace log. all= all the functions or we can specify specific function such as accept so we log in the log file only the accept functions. If you specify a function that is not relevant to the K-TAP trace log it won't log anything to the log.</p>                                                                                                                                                                                                                                                                            |
|                             | ktap_fast_tcp_verdict  | 1             | <p>For TCP connections. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: slow verdict. K-TAP sends information about the session to STAP to ask whether or not the traffic should be intercepted.</li> <li>• 1: fast verdict. K-TAP decides on its own.</li> </ul> <p>In both cases, the network/exclude network parameters are checked against the incoming IP. From 10.1.4, the value is 1 after upgrade.</p>                                                                                                                                          |
| STAP_KTAP_FAST_FILE_VERDICT | ktap_fast_file_verdict | 1             | <p>Push file information to K-TAP for determining if pipe traffic should be intercepted. For TLI connection, K-TAP sends ioctl to the S-TAP to confirm that the session is the database connection configured in the IE by checking ports and IPs, when ktap_fast_file_verdict is set to 1, then K-TAP does not send the request to the S-TAP as long as the session's ports are in the range. Valid values:</p> <ul style="list-style-type: none"> <li>• 0: disable</li> <li>• 1: enable</li> </ul> <p>Can be set when pushing to a group of DB servers via GIM.</p> |
| STAP_KTAP_BUFFER_SIZE       | ktap_buffer_size       | 4194304       | <p>Advanced. The size, in bytes, of each K-TAP buffer. Reboot the server after making changes to this parameter. Valid values: 1 MB - 32 MB</p> <p>Can be set when pushing to a group of DB servers via GIM.</p>                                                                                                                                                                                                                                                                                                                                                      |
|                             | ktap_buffer_flush      | 0             | <p>Advanced. The way to send messages from K-TAP to S-TAP. Valid values:</p> <ul style="list-style-type: none"> <li>• 1: The S-TAP reads the entire K-TAP buffer and process all the packets in the buffer</li> <li>• 0: The S-TAP reads a fixed amount rather than the entire buffer</li> </ul>                                                                                                                                                                                                                                                                      |
|                             | ktap_local_tcp         | 0             | <p>1=only intercept local connections (although previously intercepted connections are still captured) (this parameter is used for TCP connections)</p>                                                                                                                                                                                                                                                                                                                                                                                                               |
| STAP_KHASH_TABLE_LENGTH     | khash_table_length     | 24593         | <p>Length of the K-TAP table entries. Valid values: integer</p> <p>Can be set when pushing to a group of DB servers via GIM.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| GIM                                               | guard_tap.ini                            | Default value | Description                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------|------------------------------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| STAP_KHASH_M<br>AX_ENTRIES                        | khash_max_entries                        | 8192          | Maximum number of concurrent K-TAP table entries.<br>Valid values: integer<br><br>Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                |
| STAP_KTAP_FAS<br>T_SHMEM                          | ktap_fast_shmem                          | 1             | Push shmem information to K-TAP to determine if shmem traffic should be intercepted. Valid values<br><ul style="list-style-type: none"> <li>• 0: disable</li> <li>• 1: enable</li> </ul><br>Can be set when pushing to a group of DB servers via GIM.                                                                      |
| STAP_KTAP_FS<br>MON_BUFFER_<br>SIZE               | ktap_fsmon_buf<br>fer_size               | 4194304       | Advanced. Size of the K-TAP buffer for FS monitoring events, in bytes. Reboot the server after making changes to this parameter.<br>Valid values: 128 KB - 32 MB<br><br>Can be set when pushing to a group of DB servers via GIM.                                                                                          |
| STAP_ENABLE_<br>KTAP_DYNAMIC<br>_RING_BUFFER<br>S | enable_ktap_dy<br>namic_ring_buff<br>ers | 0             | Dynamically adds and removes K-TAP buffers for each main connection during peak traffic, to prevent an overflow in the K-TAP buffer. If K-TAP failover happens, data in all buffers is moved to the new buffers.<br>Valid values:<br><ul style="list-style-type: none"> <li>• 0: disabled</li> <li>• 1: enabled</li> </ul> |

Table 2. A-TAP and PCAP configuration parameters

| GIM                          | Parameter                     | Default value | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------|-------------------------------|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                              | atap_exec_locat<br>ion        | /var/guard    | Location of the executable that is used when activating A-TAP by enabling the encryption box in the inspection engine section                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                              | db_request_han<br>dler_enable | 0             | Allow the database to access K-TAP without manual configuration (requires a defined db_user in the IE section). Valid values:<br><ul style="list-style-type: none"> <li>• 0: Disabled</li> <li>• 1: Enabled</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| STAP_PCAP_RE<br>AD_TIMEOUT   | pcap_read_time<br>out         | 0             | Only PCAP traffic (non-K-TAP): PCAP packet buffer timeout, in milliseconds.<br>Do not change this value without consulting with Technical Support, after examining the problem and determining the losses (not capturing all the traffic) are caused due to PCAP/S-TAP related bottleneck.<br>Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| STAP_PCAP_DIS<br>PATCH_COUNT | pcap_dispatch_c<br>ount       | 16            | Number of PCAP packets to process at one time. Valid values:<br><ul style="list-style-type: none"> <li>• 0: process entire buffer at once.</li> <li>• positive integer: number of packets</li> </ul><br>Do not change this value without consulting with Technical Support, after examining the problem and determining that the losses (not capturing all the traffic) are caused due to PCAP/S-TAP related bottleneck.<br>Can be set when pushing to a group of DB servers via GIM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| STAP_PCAP_BU<br>FFER_SIZE    | pcap_buffer_siz<br>e          | -1            | Size of PCAP socket buffer, in kilobytes. This parameter is used for LINUX only. Valid values:<br><ul style="list-style-type: none"> <li>• -1: maximum buffer possible ( rmem_max )</li> <li>• 1-65535: buffer size in kilobytes</li> </ul><br>Larger buffer mean that it's likely to have losses when there are busts of high volume traffic. If there is a burst of high traffic, PCAP captures everything, but the S-TAP (or PCAP-to-S-TAP flow) is not fast enough and cannot keep up with the traffic. To avoid losses, the yet-to-be-processed packets are buffered. The larger the buffer is, the more resilient it is against higher and longer bursts of high traffic. Do not change this value without consulting with Technical Support, after examining the problem and determining the losses (not capturing all the traffic) are caused due to PCAP/S-TAP related bottleneck.<br>Can be set when pushing to a group of DB servers via GIM. |
|                              | pcap_backup_kt<br>ap          | 1             | When this parameter is enabled, always start PCAP regardless if ktap_installed is enabled or not, as long as there is a Db2 defined in the IE.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Linux-UNIX: S-TAP configuration per database type

This section provides detailed instructions or example for configuring monitoring on various databases.

- [Linux-UNIX: Configuring Apache Cassandra and S-TAP for auditing interception](#)  
Configure Apache Cassandra and S-TAP to monitor encrypted traffic on Apache Cassandra. Monitoring includes authorization messages for login, normal SQLs, prepared statements, batch statements, bind variables, and bound values. This configuration does not require an inspection engine or K-TAP.
- [Linux-UNIX: Application server S-TAP configuration](#)  
Application Server S-TAP is a very easy way to identify application users for Java Application Server applications when built-in functionality is not available. It doesn't require any changes to existing applications which makes it a very attractive solution. Nevertheless some considerations need to be taken into account.
- [Linux-UNIX: CockroachDB inspection engine configuration](#)  
View a typical Cockroach database inspection engine configuration. Guardium supports unencrypted connections with a cockroach database. This configuration required K-TAP.
- [Linux-UNIX: Couchbase auditing configuration](#)  
Use a double proxy to capture couchbase traffic with real client IPs.
- [Linux-UNIX: Using SAP-HANA with encrypted connections](#)  
When SAP-HANA is configured with SSL/TLS encryption, S-TAP requires configuring two proxies using NGINX.

- [Linux-UNIX: Datastax Cassandra auditing configuration](#)  
Configure logging to a file appender for monitoring encrypted traffic on Datastax Cassandra. This supports the audits provided by the built-in audit logging, for example: queries, data manipulation language, data definition language, data control syntax, authentication. This configuration does not require an inspection engine or K-TAP.
- [Linux-UNIX: Db2 IE configuration](#)  
View a typical inspection engine configuration, and flows for enabling and disabling A-TAP, and opening the SSL console for an Db2 inspection engine.
- [Linux-UNIX: Elastic Search configuration](#)  
Encrypted Elastic Search is supported via SSL termination.
- [Linux-UNIX: Configuring Exit libraries](#)  
Exit libraries embed a Guardium library into the database, using the exit mechanism. The exit library, or module, communicates directly with the Guardium S-TAP to forward database traffic.
- [Linux-UNIX: Hadoop configuration](#)  
This topic introduces fundamental concepts and processes for monitoring Hadoop data with Guardium.
- [Linux-UNIX: MongoDB IE configuration](#)  
View a typical inspection engine configuration, and flows for enabling and disabling A-TAP, and opening the SSL console for a MongoDB inspection engine.
- [Linux-UNIX: Neo4J auditing configuration](#)  
Use a double proxy together with either K-TAP or PCAP to capture encrypted Neo4J traffic.
- [Linux-UNIX: Oracle Connection Manager configuration to monitor encrypted traffic](#)  
You can use the Oracle Connection Manager to monitor encrypted traffic, without A-TAP.
- [Linux-UNIX: Oracle IE configuration](#)  
View a typical configuration for an inspection engine on an Oracle database.
- [Linux-UNIX: Configuring S-TAP interception using Oracle Unified Audit](#)  
Use Oracle Unified Auditing (OUA) to capture user activities in Oracle database environments based on Oracle Unified Audit policies. All captured activities are stored in specific tables. Linux S-TAP x86\_64 can dynamically load and use Oracle-provided libraries to connect to the configured Oracle services. The S-TAP can then pull data from the unified auditing tables, and send data to Guardium collectors.
- [Linux-UNIX: Redis configuration](#)  
Redis TCP protocol is supported by an S-TAP installed on a Redis server. If Redis is set up with SSL/TLS encryption, you need two proxies using HAProxy Load Balancer.

## Linux-UNIX: Configuring Apache Cassandra and S-TAP for auditing interception

Configure Apache Cassandra and S-TAP to monitor encrypted traffic on Apache Cassandra. Monitoring includes authorization messages for login, normal SQLs, prepared statements, batch statements, bind variables, and bound values. This configuration does not require an inspection engine or K-TAP.

### About this task

Limitations: Apache auditing does not include SOURCE\_PROGRAM, SERVER\_OS, CLIENT\_OS, DB\_PROTOCOL\_VERSION, or OS\_USER.

To configure Apache Cassandra and S-TAP for auditing, configure a logback to write to the S-TAP Cassandra audit reader in the same directory as the `guard_stap.cassandra_audit` executable. The logback is created when you enable Cassandra Audit in the S-TAP configuration. Specify the value for `cassandra_audit_delimiter` in the output string for logback.

The following jar files for this configuration are part of the S-TAP installation. They are located in the directory where the S-TAP is installed, which is often, but not always, in /usr/local/guardium/guard\_stap.

- `guardium_cassandra_audit-3.4.jar` (for the query handler, versions 3.4 to 3.10)
- `guardium_cassandra_audit-3.11.jar` (for the query handler, version 3.11 only)
- `guardium_cassandra_audit-4.0.jar` (for the query handler, versions 4.0 and higher)

The user who runs the Cassandra database must be authorized to write to the `cassandra` pipe in the S-TAP directory. Use `guardctl authorize-user` to add the user to the `Guardium` group.

When you copy the JAR files to the `cassandra` directory, make sure that the `cassandra` user has the proper permissions to read them.

Apache Cassandra auditing supports multi-tenancy.

### Procedure

1. Copy the relevant JAR files to the Cassandra lib directory so that the database can find and use them.

For example,

- Non-GIM S-TAP:

```
cp -p /usr/local/guardium/guard_stap/guardium_cassandra_audit-4.0.jar /usr/share/cassandra/lib
```

- GIM S-TAP:

```
cp -p /usr/local/modules/STAP/current/guardium_cassandra_audit-4.0.jar /usr/share/cassandra/lib
```

2. Enable Cassandra auditing in S-TAP by setting the `cassandra_audit_enabled=1`. You can set this parameter from the GUI, by editing the `guard_tap.ini` file, or by using the `update_stap_config` grdapi function.

3. Authorize the `cassandra` user to write to the Cassandra pipe in the S-TAP directory.

For example,

- Non-GIM S-TAP:

```
/usr/local/guardium/guard_stap/guardctl --db-user=cassandra authorize-user
```

- GIM S-TAP:

```
/usr/local/guardium/modules/ATAP/current/files/bin/guardctl -db-user=cassandra authorize-user
```

4. Edit the `logback.xml` configuration file as shown in the following example.

```

<appender name="Guardium" class="ch.qos.logback.core.FileAppender">
<file>/usr/local/guardium/guard_stap/.cassandra_audit</file>
<immediateFlush>true</immediateFlush>
<encoder>
<pattern>%msg{}GUARD_DELIM</pattern>
</encoder>
</appender>
<logger name="com.ibm.guardium" level="INFO">
<appender-ref ref="Guardium"/>
</logger>

```

- Non-GIM S-TAP:

```
<file>/usr/local/guardium/guard_stap/.cassandra_audit</file>
```

- GIM S-TAP:

```
<file>/usr/local/modules/STAP/current/.cassandra_audit</file>
```

5. Change jvm.options to enable the custom\_query\_handler\_class to call into the logging mechanism by setting JVM\_EXTRA\_OPTS to include the following line.

```
-Dcassandra.custom_query_handler_class=com.ibm.guardium.CassandraQueryHandler
```

6. To enable AUTH logging on, when users connect to the database, set a property in JVM\_EXTRA\_OPTS so that the logging mechanism can correctly redirect auth requests.

For example, if you use PasswordAuthenticate, add the following statement to JVM\_EXTRA\_OPTS.

```
-DGardiumBaseAuthenticator=org.apache.cassandra.auth.PasswordAuthenticator
```

Then, instead of specifying PasswordAuthenticator in cassandra.yaml, you can use com.ibm.guardium.CassandraAuthenticator.

7. The default role manager (CassandraRoleManager) explicitly checks for PasswordAuthenticator. Therefore, if you enable AUTH logging, you also need to change role\_manager in cassandra.yaml.

Set role\_manager to com.ibm.guardium.GuardCassandraRoleManager and specify an additional property in JVM\_EXTRA\_OPTS for the role manager to use.

For example, -DGardiumBaseRoleManager=org.apache.cassandra.auth.CassandraRoleManager

8. Set Java environment variables. For example,

```
JVM_OPTS="$JVM_OPTS $JVM_EXTRA_OPTS"
```

## What to do next

Optionally, you can choose to decode the username during a failed login. To add the decoding functionality, use a class that can understand the format that you are using. Since Cassandra can be extended to use custom authenticators, this format might differ from the base PasswordAuthenticator, which uses SASL. Guardium provides a decoder that works for PasswordAuthenticator. You can optionally switch out the decoder for PasswordAuthenticator for a different decoder, which must be provided by the implementor of the custom authenticator. To specify the replacement decoder, add the following to JVM\_EXTRA\_OPTS (default-included decoder for PasswordAuthenticator shown): -DGardiumBaseAuthenticatorDecoder=com.ibm.guardium.GuardPasswordAuthenticatorDecoder. The interface for the replacement authenticator is as follows,

```

package com.ibm.guardium;
import java.nio.ByteBuffer;
public interface IGuardAuthenticatorDecoder
{
 String getUsername(byte[] clientResponse);
}

```

## Linux-UNIX: Application server S-TAP configuration

Application Server S-TAP is a very easy way to identify application users for Java Application Server applications when built-in functionality is not available. It doesn't require any changes to existing applications which makes it a very attractive solution. Nevertheless some considerations need to be taken into account.

For Application Server S-TAP to work, the username needs to be transmitted in clear text in the HTTP stream. Some authentication mechanisms, for example, regular HTTP based authentication are hashed or Base64 encoded and are not supported. In general Form Logins transmit the username in clear text.

This method does not work with all applications. It depends on the way that connection pooling is used. For example, it requires that the access to the database is synchronous with the same process or thread that is handling the HTTP request. A good example is a servlet-based application where a servlet processes HTTP requests, and in the process receives a connection from a connection pool to access the database.

HTTPS connections are also not supported. This is normally not a crucial problem because the S-TAP is installed on the application server. In normal enterprise configurations, only traffic to the web server is HTTPS encrypted and the connection between web and application server is standard HTTP.

There are situations when it is not possible or desirable to change the application source code, so the Guardium Application Event API cannot be used. The application may also not use stored procedures to define user boundaries. In some of these cases the ability of the Guardium S-TAP to monitor network traffic can be used to identify application users. In this scenario the S-TAP is used to correlate application end users with database activity. An S-TAP is installed on the machine that hosts the application server; and is not installed on the machine that hosts the database server. It is then configured to monitor incoming HTTP traffic to the application server, filter out user names and correlate them through an application server session id with database activity. In Guardium this is called Application Server User Identification or Application Server S-TAP.

This approach is advantageous because it works without changing the application or reconfiguring the application server. It is therefore a very fast and easy solution. The disadvantages are that it also does not work with all enterprise applications. Possible problems include incompatible authentication mechanisms that encrypt or hash user names. Application Server S-TAP works best for standard Java Enterprise Applications using a type of Form Login authentication.

1. Analyze the application's web traffic to determine:

- The HTTP port of the application server.
- The application user name in the HTTP traffic during login.
- The Java Session ID that is correlated to the user name.

There are various tools you can use for this analysis. It is beyond the scope of the Guardium Knowledge Center.

## 2. Configure and save the Application server S-TAP. Typical parameter values specific for the application server settings:

- App. Server User Identification: 1
- App server user ID: 1
- Session timeout:1800
- Ports: 8081
- Login pattern: userid
- Username prefix: userid=
- Username postfix: &
- Session pattern: action=login
- Session prefix: JSESSIONID=
- Session postfix: ;
- Session ID pattern: Cookie
- Session ID prefix: USESESSIONID=
- Session ID postfix: ;

Guardium stores the application username in the field **Application User**, in the entity **Access Period**. You can add this field to reports.

## Related reference

- [Linux-UNIX: Application server parameters](#)

## Linux-UNIX: CockroachDB inspection engine configuration

View a typical Cockroach database inspection engine configuration. Guardium supports unencrypted connections with a cockroach database. This configuration required K-TAP.

```
[DB_0]
connect_to_ip=127.0.0.1,::1
db2_fix_pack_adjustment=20
db2_shmem_client_position=0
db2_shmem_size=131072
db2bp_path=NULL
db_exec_file=NULL
db_install_dir=NULL
db_type=cockroach
db_user=NULL
encryption=0
db_version=0
instance_running=1
intercept_types=NULL
load_balanced=1
port_range_end=25258
port_range_start=25257
priority_count=20
real_db_port=25257
tap_identifier=cockroach_snif-cockrach01(25257,25258,DB_0)
unix_domain_socket_marker=PGSQL
networks=0.0.0.0/0.0.0.0,::/0
exclude_networks=
```

## Linux-UNIX: Couchbase auditing configuration

Use a double proxy to capture couchbase traffic with real client IPs.

## About this task

This procedure requires two proxies of either Nginx or HAProxy type. Both must be located on the database.

### Guidelines:

- Incoming encrypted traffic from the Client is sent to the first proxy instance, Proxy1.
- Proxy1 terminates the SSL and adds the proxy protocol to ports.
- The second proxy instance, Proxy2, listens to intermediate ports and removes the proxy protocol.
- K-TAP intercepts traffic in between Proxy1 and Proxy2 to get decrypted traffic with real client IPs.
- Outgoing decrypted traffic from Proxy2 is sent to unencrypted Couchbase database ports.

## Procedure

### 1. Configure the database.

These ports must be open on each host for Couchbase Server to operate correctly. In addition, these ports must be available (not blocked by a firewall or other such mechanism):

- Between each node of a cluster
- Between nodes of multiple clusters connected by using XDCR
- Between application servers and nodes, and for administrative access

| Port Name                              | Default Port Number<br>Unencrypted /<br>Encrypted | Description                         | Node-to-node | Client-to-Node | Cluster admin | XDCR v1 (CAPI) | XDCR v2<br>(XMEM) |
|----------------------------------------|---------------------------------------------------|-------------------------------------|--------------|----------------|---------------|----------------|-------------------|
| rest_port /<br>ssl_rest_port           | 8091 / 18091                                      | REST/HTTP<br>including web UI       | Yes          | Yes            | Yes           | Yes            | Yes               |
| capi_port /<br>ssl_capi_port           | 8092 / 18092                                      | Views and XDCR<br>access            | Yes          | Yes            | No            | Yes            | Yes               |
| query_port /<br>ssl_query_port         | 8093 / 18093                                      | Query service<br>REST/HTTP traffic  | Yes          | Yes            | No            | No             | No                |
| fts_http_port /<br>fts_ssl_port        | 8094 / 18094                                      | Search service<br>REST/HTTP traffic | Yes          | Yes            | No            | No             | No                |
| memcached_port /<br>memcached_ssl_port | 11210 / 11207                                     | Data Service                        | Yes          | Yes            | No            | No             | Yes               |

2. Proxy Configuration: There are two ways to setup Proxy configurations along with IPTABLE configurations.

- Proxy1 listens on port 1xxxx, so external ports are still the same to the user. For example, an encrypted connection still connects via the GUI as `http://COUCHBASE:1xxxx`. In this case the couchbase configuration needs to make sure it is not listening on 1xxxx. Couchbase configuration is in the `static_config` file. To avoid reconfiguring clients, the default ports must be modified so that the clients connect to the first proxy instance instead. For example:

```
{memcached_ssl_port, 11207}
{ssl_rest_port, 18091}
{ssl_capi_port, 18092}
{ssl_query_port, 18093}
{fts_ssl_port, 18094}
```

These ports need to be used in the first proxy instance and Couchbase would need to be configured to expect unencrypted connections and to move these ports to a different number so that they do not duplicate ports being listened on by the proxy instances.

- Proxy1 listens on port yxxxx where y is not 1, so the couchbase configuration can stay as the default, but external ports need to be changed to yxxxx.

3. Configure HAProxy. (Not required if you are using NGINX.)

To enable Proxy Protocol in HAProxy1, add the `send-proxy` keyword to the `/etc/haproxy/haproxy.cfg` file. To get the Real Client IP, strip the Proxy protocol in HAProxy2, and add `accept-proxy` to `/etc/haproxy/haproxy.cfg` file.

Added/Modify `haproxy.cfg` for all couchbase ssl ports, giving an example of ssl port(1xxxx), where xxxx is SSL port, such as 8091/8092, etc; yyy is service name such as rest/capi/query, etc.

Method1: Proxy1 listens on port 1xxxx and pass traffic to Proxy2, Proxy2 listens on port 2xxxx and send decrypted traffic to couchbase no ssl port (xxxx). By using this method, couchbase should not listen on port 1xxxx.

- frontend yyy\_in bind \*:

```
bind *:1xxxx ssl crt /etc/haproxy/ha_couchbase_cert_key.pem
default_backend send_pp_yyy
```

- backend send\_pp\_yyy

```
balance roundrobin
server intermediate_yyy 127.0.0.1:2xxxx send-proxy
```

- frontend strip\_pp\_yyy

```
bind 127.0.0.1:2xxxx accept-proxy
default_backend yyy_out
```

- backend yyy\_out

```
balance roundrobin
server yyyy 127.0.0.1:xxxx
```

Method2: Proxy1 listens on port 3xxxx and passes traffic to Proxy2. Proxy2 listens on port 2xxxx and sends decrypted traffic to couchbase no ssl port (xxxx). By using this method, the external port for user should be changed to 3xxxx.

- frontend yyy\_in bind \*:

```
bind *:3xxxx ssl crt /etc/haproxy/ha_couchbase_cert_key.pem
default_backend send_pp_yyy
```

- backend send\_pp\_yyy

```
balance roundrobin
server intermediate_yyy 127.0.0.1:2xxxx send-proxy
```

- frontend strip\_pp\_yyy

```
bind 127.0.0.1:2xxxx accept-proxy
default_backend yyy_out
```

- backend yyy\_out

```
balance roundrobin
server yyyy 127.0.0.1:xxxx
```

4. Configure NGINX. (Not required if you are using HAProxy.)

For a TCP stream, the PROXY protocol can be enabled for connections between NGINX and an upstream server. To enable the PROXY protocol in Nginx1, include the `proxy_protocol` directive in a server block at the stream {} level in `/etc/nginx/nginx.conf`. NGINX terminates HTTPS traffic (the `ssl_certificate` and `ssl_certificate_key` directives) and proxies the decrypted data to a backend server. In Nginx2, add listen with `proxy_protocol` to receive the client's real IP forwarded with Proxy Protocol.

- a. Make sure that your NGINX installation includes the HTTP and Stream Real IP modules:

```
nginx -V 2>&1 | grep -- 'http_realip_module'
nginx -V 2>&1 | grep -- 'stream_realip_module'
```

b. Add/modify nginx.cfg for all couchbase ssl ports, giving an example of ssl port(1xxxx), where xxxx is SSL port, such as 8091/8092, etc; yyy is service name such as rest/capi/query, etc.

- Method1: Proxy1 listens on port 1xxxx and pass traffic to Proxy2, Proxy2 listens on port 2xxxx and sends decrypted traffic to couchbase no ssl port (xxxx). When using this method, couchbase should not listen on port 1xxxx.

```
stream {
 server {
 listen 1xxxx ssl;
 proxy_pass 127.0.0.1:2xxxx;
 ssl_certificate /opt/couchbase/SSLCA/chain.pem;
 ssl_certificate_key /opt/couchbase/SSLCA/nodedir/pkey.key;
 ssl_session_cache shared:SSL:8m;
 proxy_protocol on;
 }

 server {
 listen 2xxxx proxy_protocol;
 proxy_pass 127.0.0.1:xxxx;
 }
}
```

- Method2: Proxy1 listens on port 3xxxx and pass traffic to Proxy2, Proxy2 listens on port 2xxxx and send decrypted traffic to couchbase no ssl port (xxxx). When using this method, the external port for user should be changed to 3xxxx.

```
stream {
 server {
 listen 2xxxx ssl;
 proxy_pass 127.0.0.1:3xxxx;
 ssl_certificate /opt/couchbase/SSLCA/chain.pem;
 ssl_certificate_key /opt/couchbase/SSLCA/nodedir/pkey.key;
 ssl_session_cache shared:SSL:8m;
 proxy_protocol on;
 }

 server {
 listen 3xxxx proxy_protocol;
 proxy_pass 127.0.0.1:xxxx;
 }
}
```

##### 5. Configure the network.

If the client is on the same server with the DB, verify that all traffic from the client is sent to Proxy1. Otherwise, all traffic that is not from Proxy2 to DB is dropped. This requires IPTABLE setup.

In order to support encrypted traffic for couchbase, it is necessary to configure a proxy service to terminate the encryption. The proxy solution that is used depends on your requirements, though NGINX and HAProxy both work well for this. [Example configurations are attached above]

Using this script to setup IPTABLES. The UID can vary depending on your system configuration. As with all firewall rules, order is important.

```
#!/bin/sh

Remove any existing jumps to our custom chains
iptables -D INPUT -j chain-couchbase-incoming
iptables -D OUTPUT -j chain-couchbase-outgoing

Clean any existing custom chains
iptables -F chain-couchbase-incoming
iptables -F chain-couchbase-outgoing
iptables -X chain-couchbase-incoming
iptables -X chain-couchbase-outgoing
iptables -N chain-couchbase-incoming
iptables -N chain-couchbase-outgoing

Define external(proxy1), proxy2, ssl and no ssl ports
external_port_prefix=0
ssl_port_prefix=0
proxy2_port_prefix=0
port_list=0

Pass in all arguments, please see bottom usage.
for i in "$@" ; do
 # set the port prefix
 if echo $i | grep '^-' > /dev/null; then
 if echo $i | grep '^external_port_prefix$' > /dev/null; then
 external_port_prefix=999
 elif echo $i | grep '^ssl_port_prefix$' > /dev/null; then
 ssl_port_prefix=999
 elif echo $i | grep '^port_list$' > /dev/null; then
 port_list=999
 fi
 elif ["X$external_port_prefix" = "x999"]; then
 external_port_prefix=$i
 elif ["X$proxy2_port_prefix" = "x999"]; then
 proxy2_port_prefix=$i
 elif ["X$ssl_port_prefix" = "x999"]; then
 ssl_port_prefix=$i
 elif ["X$port_list" = "x999"]; then
 port_list=$i
 fi
 # set ports
 if ["$i" = "11210"]; then
 external_port=${external_port_prefix}1207
 proxy2_port=${proxy2_port_prefix}1207
```

```

 ssl_port=${ssl_port_prefix}1207
else
 external_port=${external_port_prefix}${i}
 proxy2_port=${proxy2_port_prefix}${i}
 ssl_port=${ssl_port_prefix}${i}
fi

#####
INCOMING RULES

Allow loopback access to intermediate ports so that proxy1 can
route traffic to proxy2
iptables -A chain-couchbase-incoming -i lo -p tcp --dport ${proxy2_port} -j ACCEPT

Disallow external access to proxy2
iptables -A chain-couchbase-incoming -p tcp --dport ${proxy2_port} -j REJECT

Disallow direct access to encrypted ports
iptables -A chain-couchbase-incoming -p tcp --dport ${ssl_port} -j REJECT

Allow loopback access to unencrypted ports so that proxy2 can
route traffic to DB
iptables -A chain-couchbase-incoming -i lo -p tcp --dport ${i} -j ACCEPT

Disallow direct access to unencrypted ports
iptables -A chain-couchbase-incoming -p tcp --dport ${i} -j REJECT

Allow access to proxy1
iptables -A chain-couchbase-incoming -p tcp --dport ${external_port} -j ACCEPT

#####
OUTGOING RULES

Allow loopback access to unencrypted ports to allow routing from proxy2 to
DB (proxy2 runs under couchbase UID)
iptables -A chain-couchbase-outgoing -o lo -p tcp --dport $i -m owner --uid couchbase -j ACCEPT

Allow loopback access to intermediate ports to allow routing from proxy1 to
proxy2 (proxy1 runs under couchbase UID)
iptables -A chain-couchbase-outgoing -o lo -p tcp --dport ${proxy2_port} -m owner --uid couchbase -j ACCEPT

Disallow loopback access to unencrypted ports to prevent local clients from
skipping interception
iptables -A chain-couchbase-outgoing -o lo -p tcp --dport $i -j REJECT
fi
done

if ["${port_list}" = "0"]; then
 echo "usage: /root/set_firewall.sh -external_port_prefix [1-9] -proxy2_port_prefix[1-9] -ssl_port_prefix [1-9] -
port_list [servers's no SSL port list]"
 echo "for example /root/set_firewall.sh -external_port_prefix 2 -proxy2_port_prefix 3 -ssl_port_prefix 1 -port_list
8091 8092 8093 8094 11210"
fi

Firewall chains need to return at the end
iptables -A chain-couchbase-incoming -j RETURN
iptables -A chain-couchbase-outgoing -j RETURN

Hook the main rules up to the chains
iptables -A INPUT -j chain-couchbase-incoming
iptables -A OUTPUT -j chain-couchbase-outgoing

```

#### 6. Configure the S-TAP.

Use the first instance of the proxy to terminate the encryption and add proxy-protocol for Guardium to collect the traffic and be able to attribute the correct analyzed\_client\_ip. Use the second instance to remove proxy-protocol, in order to not break the connection to the database. Configure the inspection engine to collect the traffic between the two proxy instances. For example, if you are using the sample configurations above, then the ports to collect for Couchbase are 28091-28094, 11210, 21207. If local TCP connections are allowed, then iptables rules need to allow for the possibility that the UID can vary depending on your system configuration. And as with all firewall rules, order is important.

Edit the inspection engine for port\_range\_end, port\_range\_start and real\_db\_port. They should be set as proxy2 port or range and db\_type should be COUCHBASE. For example, when proxy2 port is 2xxxx:

- If you are using K-TAP, modify the IE parameters in the guard\_tap.ini file:

```
[DB_0]
db_type=COUCHBASE
port_range_end=28094
port_range_start=28091
real_db_port=28091
networks=127.0.0.1/255.255.255.255,9.70.165.199/255.255.255.255
```

- If you are using PCAP, modify the parameters in the guard\_tap.ini file:

```
devices=ens32,lo
ktap_installed=0

[DB_0]
db_type=COUCHBASE
port_range_end=28094
port_range_start=28091
real_db_port=28091
```

---

## Linux-UNIX: Using SAP-HANA with encrypted connections

When SAP-HANA is configured with SSL/TLS encryption, S-TAP requires configuring two proxies using NGINX.

## Before you begin

---

Verify the following prerequisites:

- S-TAP is installed and configured on the SAP-HANA server.
- NGINX is installed and configured for reverse-proxy connections.
- SAP-HANA is configured to use only SSL/TLS connections and the database global configuration enforces SSL/TLS. For example:

```
[communication]
ssl = on
sslEnforce = true
```

## Procedure

---

1. Identify the ports clients use to connect to the database.
2. Configure NGINX using the configuration file that is typically located at `/etc/nginx/nginx.conf`.

For example, assuming that the original port for client connections to the database is 30015 and the SSL certificate is `sap-hana.pem`:

```
worker_processes 1;

load_module lib64/nginx/modules/ngx_stream_module.so;

events {
 worker_connections 1024;
 use epoll;
}
stream {
 upstream saphana {
 server localhost:30015;
 }

 server {
 listen 31015 ssl;
 proxy_pass localhost:32015;
 proxy_protocol on;
 ssl_certificate /hana/shared/HXE/HDB00/su12u2ppc64le-hana/sec/sap-hana.pem;
 ssl_certificate_key /hana/shared/HXE/HDB00/su12u2ppc64le-hana/sec/sap-hana.key;
 }
 server {
 listen 32015 proxy_protocol;
 proxy_pass saphana;
 proxy_ssl on;
 proxy_ssl_certificate /hana/shared/HXE/HDB00/su12u2ppc64le-hana/sec/sap-hana.pem;
 proxy_ssl_certificate_key /hana/shared/HXE/HDB00/su12u2ppc64le-hana/sec/sap-hana.key;
 }
}
```

3. Restart the NGINX service using the following command: `sudo systemctl restart nginx`.

4. Configure the S-TAP for SAP-HANA using second proxy port.  
For example, in a typical inspection engine configuration:

```
[DB_0]
connect_to_ip=127.0.0.1,::1
db2_fix_pack_adjustment=20
db2_shmem_client_position=61440
db2_shmem_size=131072
db2bp_path=NULL
db_exec_file=NULL
db_install_dir=NULL
db_user=NULL
db_type=HANA
encryption=0
informix_inf_file=NULL
db_version=
instance_running=1
intercept_types=NULL
load_balanced=1
port_range_end=32050
port_range_start=32010
priority_count=20
real_db_port=32015
tap_identifier=SAP-HANA
tee_listen_port=0
unix_domain_socket_marker=NULL
networks=0.0.0.0/0.0.0.0,::/0
exclude_networks=
```

Note: If clients use multiple ports for database connections, the NGINX configuration file requires multiple reverse-proxy sections.

## Linux-UNIX: Datastax Cassandra auditing configuration

---

Configure logging to a file appender for monitoring encrypted traffic on Datastax Cassandra. This supports the audits provided by the built-in audit logging, for example: queries, data manipulation language, data definition language, data control syntax, authentication. This configuration does not require an inspection engine or K-TAP.

## Before you begin

---

See [Datastax online reference](#) for details about Datastax audit logging.

The user running the Cassandra database needs to be authorized to write to the cassandra pipe in the S-TAP directory. Use guardctl authorize-user to add the user to the group.

Before copying the jars to the Cassandra directory, make sure that the Cassandra user has appropriate permissions to read the jar files.

## About this task

---

Datastax Cassandra auditing can be configured concurrently with Apache Cassandra on the same host, since they have different setups on different files. The S-TAP handles both of them similarly, via a pipe.

Datastax Cassandra auditing supports multi-tenancy.

## Procedure

---

1. On the database, open the file dse.yaml in a text editor and update the Audit logging options section, with:

```
Audit logging options
audit_logging_options:
 enabled: true
 logger: SLF4JAuditWriter
```

2. Save and close the file.

3. Open the file logback.xml in a text editor and add this appender:

```
<appender name="GuardiumAuditWriterAppender" class="ch.qos.logback.core.FileAppender">
 <file>S-TAP location in your system</file>
 <encoder>
 <pattern>%msg{}GUARD_DELIM</pattern>
 <immediateFlush>true</immediateFlush>
 </encoder>
</appender>
```

Typical S-TAP locations are:

- non-GIM installations: /usr/local/guardium/guard\_stap/
- GIM installations: /opt/modules/STAP/current/

4. Add the new appender to audit logger:

```
<logger name="SLF4JAuditWriter" level="INFO" additivity="false">
 <appender-ref ref="SLF4JAuditWriterAppender"/>
 <appender-ref ref="GuardiumAuditWriterAppender"/>
</logger>
```

5. Save and close the file.

6. Verify that the guard\_tap.ini parameter cassandra\_audit\_enabled=1.

This creates the file appender pipe for Cassandra/Datastax with native audit logging.

7. If the guard\_tap.ini parameter cassandra\_audit\_delimiter if set to something other than the default, verify that the value "GUARD\_DELIM" in the logger configuration has the same value.

8. On your Guardium system, add the Cassandra user to the "guardium" group, by entering:

```
/usr/local/guardium/guard_stap/guardctl authorize-user <cassandra>
```

This allows the Cassandra user to write to the pipe file appender. The permissions on the pipe allow the S-TAP user to read/write and anyone in the guardium group to write.

9. Restart theS-TAP to create the Cassandra audit pipe.

10. Restart the Cassandra instance to pick up the logging changes. (The restart for Cassandra also ensures that the guardium group membership is picked up for the new Cassandra process.)

## Related reference

---

- [Linux-Unix: General parameters](#)

## Linux-UNIX: Db2 IE configuration

---

View a typical insepction engine configuration, and flows for enabling and disabling A-TAP, and opening the SSL console for an Db2 inspection engine.

## Typical Db2 inspection engine configuration

---

```
name =db24
type =db2
sequence =4
connect to IP=127.0.0.1
install dir = /home/db2inst1
exec file = /home/db2inst1/sqllib/adm/db2sysc
encrypted = no
port range = 50000 - 50000
ktap real port = 50000
identifier = db2_9.32.164.228(50000,50000,DB_3)
client = 0.0.0.0/0.0.0.0
```

## Activate and deactivate A-TAP for SSL traffic

---

Before activating A-TAP, you need to stop the Db2 instance:

```
systemctl stop db2
```

Activate A-TAP:

```
/usr/local/guardium/guard_stap/guardctl --db-user=db2 --db-type=oracle --db-instance=db2 --db-base=/home/ibmuser --db-home=/usr db2
```

Restart the Db2 instance:

```
systemctl start db2
```

## Set up Db2 with TLS/SSL certificate and key

---

For example, on an instance with SSL and kerberization:

### Deactivating A-TAP

---

Before deactivating A-TAP, you need to stop the Db2 instance.

```
systemctl stop db2
```

Deactivate A-TAP: Restart the Db2 instance:

```
systemctl start db2
```

---

## Linux-UNIX: Elastic Search configuration

Encrypted Elastic Search is supported via SSL termination.

Configuration guidelines:

- Elastic Search is configured to listen on the loopback device only, allowing the SSL termination to occur on the public interface.
- Elastic search uses a PKCS12 file that needs to be converted to PEM; and private key files for NGINX to use.
- In this example, the IE is configured to capture traffic on port 9201. The traffic enters the system encrypted on public port 9200, gets decrypted and routed to port 9201, then re-encrypted and passed to the loopback port 9200 where it is handled by Elastic Search.

An example configuration for Elastic Search for NGINX:

```
[root@<elasticsearch host> ~]# cat /etc/nginx/nginx.conf
user elasticsearch;
worker_processes 1;
error_log /var/log/nginx/error.log warn;
pid /var/run/nginx.pid;
events {
 worker_connections 1024;
}
http {
 server {
 listen 9201;
 server_name <elasticsearch hostname>;
 location / {
 proxy_ssl_certificate /usr/share/elasticsearch/config/<elasticsearch hostname>.crt;
 proxy_ssl_certificate_key /usr/share/elasticsearch/config/<elasticsearch hostname>.key;
 proxy_pass https://localhost:9200;
 proxy_http_version 1.1;
 }
 }
 server {
 listen <elasticsearch host>:9200 ssl;
 server_name <elasticsearch host>;
 ssl_certificate /usr/share/elasticsearch/config/<elasticsearch hostname>.crt;
 ssl_certificate_key /usr/share/elasticsearch/config/<elasticsearch hostname>.key;
 location / {
 proxy_pass http://<elasticsearch hostname>:9201;
 proxy_http_version 1.1;
 }
 }
}
[root@<elasticsearch hostname> ~]#
```

Typical inspection engine configuration:

```
[DB_0]
connect_to_ip=127.0.0.1::1
db2_fix_pack_adjustment=20
db2_shmem_client_position=0
db2_shmem_size=131072
db2bp_path=NULL
db_exec_file=NULL
db_install_dir=NULL
db_type=EL_SEARCH
db_user=elastic
encryption=0
```

```

db_version=9
instance_running=1
intercept_types=NULL
load_balanced=1
port_range_end=9201
port_range_start=9201
priority_count=20
real_db_port=9201
tap_identifier=el_search_9.98.176.129(9300,9300,DB_0)
tee_listen_port=0
unix_domain_socket_marker=NULL
networks=0.0.0.0/0.0.0.0,:::/0
exclude_networks=

```

## Linux-UNIX: Configuring Exit libraries

Exit libraries embed a Guardium library into the database, using the exit mechanism. The exit library, or module, communicates directly with the Guardium S-TAP to forward database traffic.

- [Linux-UNIX: Configuring Db2, Informix, and Teradata exit by using the setup\\_exit.sh script](#)  
Run the setup\_exit.sh script to configure and activate the Db2, Informix, and Teradata exit libraries. The script makes all of the configuration updates in both the database and the S-TAP.
- [Linux-UNIX: Configuring Db2 Exit](#)  
The Db2® Exit module enables S-TAP to monitor any Db2 database activities, whether encrypted or not and whether local or remote. It does not require A-TAP or K-TAP.
- [Linux-UNIX: Configuring Informix Exit](#)  
The Informix exit module enables S-TAP to monitor any Informix database activities, whether encrypted or not and whether local or remote. It does not require A-TAP or K-TAP.
- [Linux-UNIX: Configuring Teradata exit](#)  
The Teradata exit module enables S-TAP to monitor any Teradata database activities, whether encrypted or not and whether local or remote. It does not require A-TAP or K-TAP.

## Related concepts

- [Embedded integrations](#)

## Linux-UNIX: Configuring Db2, Informix, and Teradata exit by using the setup\_exit.sh script

Run the setup\_exit.sh script to configure and activate the Db2, Informix, and Teradata exit libraries. The script makes all of the configuration updates in both the database and the S-TAP.

### Before you begin

- Make sure you know the database username.
- The inspection engine for the exit library must be configured on the database. Use one of the following methods:
  - During S-TAP installation, if auto-discovery is enabled, it auto-discovers databases and creates inspection engines for the discovered databases.
  - [Linux-UNIX: S-TAP Control: Inspection engine parameters](#)
  - [Linux-UNIX: Configuring an Inspection Engine](#)

### About this task

The setup\_exit.sh script is part of the S-TAP installation, and is located in the S-TAP installation directory. This script is an alternative to the exit configuration tasks described in [Linux-UNIX: Configuring Db2 Exit](#), [Linux-UNIX: Configuring Informix Exit](#), [Linux-UNIX: Configuring Teradata exit](#), which describe the full configuration of each exit.

If this database is the only one to monitor, then K-TAP is not required. Set ktap\_installed=0 in guard\_tap.ini, or with GIM set ktap\_enabled to no. However, if another database (DB\_TYPE is not EXIT) needs monitoring by S-TAP, then K-TAP is required.

### Procedure

1. Log in to the database server as **root**, and access the S-TAP installation directory.
2. Run `./setup_exit.sh [db2 | informix | teradata]`  
The script starts to run, and prompts you for the required details. When you complete the script, the system responds with a message similar to one of:
  - If the configuration is valid: DB <db user> has a GOOD setup for EXIT.
  - If you skipped something in the configuration: <xxx> is skipped, <yyy> will not work. This message indicates that the inspection engine is not properly configured for the type of exit library.
  - If the inspection engine is not an exit inspection engine, or not a specified DB type, the script skips the inspection engine, and a message is logged as Section \${db\_section} is not target IE, skip
  - If the script setup needs an S-TAP restart: To work with EXIT, please restart STAP!!.
  - If the script setup needs a database restart: Please restart the <db\_type> (<db\_user>) !!, for example a DB2 with db\_user of db2inst1 Please restart the DB2 (db2inst1) !!.
3. Optional: Set up Zone or WPARs.
  - a. In the secondary zone or WPAR, install the same version of S-TAP that is already installed in global, with K-TAP disabled.

- b. On the zone or WPAR, add the exit inspection engine in the guard\_tap.ini or configure by using the GUI.
- c. If discovery automatically created any inspection engines for zones or WPARs on the global zone, delete them.

## Linux-UNIX: Configuring Db2 Exit

The Db2® Exit module enables S-TAP to monitor any Db2 database activities, whether encrypted or not and whether local or remote. It does not require A-TAP or K-TAP.

### About this task

Db2 Exit embeds a Guardium® library into the Db2 database and communicates with the S-TAP with a Guardium shared library.

By default, Guardium supports up to 10 total Exit inspection engines (combined total of all Exit types). If you use more than one type of Exit, the combined maximum is 10. For more information, see the [exit\\_libs\\_num\\_threads](#) parameter in [Linux-UNIX: General parameters](#).

Db2 Exit shared libraries are part of the Guardium UNIX S-TAP installation. S-TAP includes 64-bit and 32-bit.

- libguard\_db2\_exit\_64.so
- libguard\_db2\_exit\_32.so (available for RHEL6 on the i686 CPU only)

When you install the S-TAP, it copies libraries in the standard library paths, and creates links.

- The S-TAP copies libraries in the standard library paths:
  - Shell Installation - <guardium\_installation\_directory>/guard\_stap
  - GIM Installation - < guardium\_installation\_directory>/modules/STAP/current/files
- And then creates links. For example:
  - /usr/lib64/libguard\_db2\_exit\_64.so -> libguard\_db2\_64.so.<release number>
  - /usr/lib/libguard\_db2\_exit\_32.so -> libguard\_db2\_32.so.<release number>

The digits after `.so`, reflect the release number. These digits were introduced in V10.6. (In previous releases, Lib files do not include release numbers.)  
[Guardium support matrix](#) details exactly what Db2 Exit can monitor.

If you are not monitoring another database, then K-TAP is not required. Set ktap\_installed=0 in `guard_tap.ini`, or with GIM; set ktap\_enabled to no. You can upgrade the Linux OS and the S-TAP without being concerned about K-TAP module compatibility. However, if you are monitoring another database with S-TAP, then K-TAP is required. Ensure that a compatible K-TAP module is available when you upgrade your Linux version.

When you upgrade S-TAP from 10.6.0.0 and higher, database restart is not required. You can upgrade S-TAP while the database is running. The EXIT library from the previous version is used until you restart the database. When you restart the database, it starts by using the updated exit library on the S-TAP. However, if the new library addresses any issues you are waiting for, you must restart the database.

Use the Db2 Exit health check script to gather information from the Db2 server when you configure the Db2 inspection engines. The script is located in the `guard_stap/bin` directory. You can run it from anywhere with the full path. The script name is `./db2_exit_health_check.sh [ check | fix ]`. By default it outputs some of the IE parameters for each DB2\_EXIT inspection engine, and runs checks on the IE configuration. Use the fix option to fix the IE parameters.

**User authorization:** The user must be authorized for the `guardium` group. If the `guardium` group was created in LDAP, then take one of the following steps,

- Create a local group called `guardium` with the same group ID (when you authorize the DB user it is added to this group).
- Add the `guardium` group ID (GID) to the DB user in `/etc/passwd`.

In a shell installation, if the inspection engine `db_user` is specified, then you don't need to authorize the user even in an LDAP environment.

In a GIM installation, you still need to authorize the db user.

Note: If your site uses Db2 Warehouse, you can use the Db2 Warehouse integration. For more information, see [Embedded integrations](#).

## Procedure

1. Install and start the S-TAP agent on the database server and configure an Inspection engine for the `db2_exit` protocol. See [Linux-UNIX: Before you start installing S-TAP](#) and [Linux-UNIX: Inspection engine parameters](#).
2. If S-TAP is already installed and configured with A-TAP:
  - a. Stop the Db2 by entering `db2stop force; ipclean`
  - b. Deactivate the A-TAP by entering `/opt/IBM/guardium/module/modules/ATAP/current/files/bin/guardctl db_instance=<db_instance> deactivate`
  - c. Configure the IE (Inspection Engine) for DB2\_EXIT as usual either in the `guard_tap.ini` or from the GUI. (Make sure any previously configured IE for `db_type=DB2_EXIT` is removed.)
  - d. Verify that the parameter `db_install_dir` for DB2\_EXIT IE is set to the value of `$DB2_HOME` or `$HOME` of Db2 environment variable.
  - e. Restart the S-TAP with the new configuration.
3. Determine the bitwise of the Db2. Log in as `root` and run `db2level`. The output is similar to  
`DB21085I Instance db2inst1 uses 64 bits and DB2 code release SQL09070, with level identifier 08010107`
4. Locate the communication buffer exit library location (DB2PATH):
  - a. Log in to Db2 as user `trip`
  - b. In the Db2 CLP, run `get database manager configuration`
  - c. In the output, look for default database path:  
`Default database path (DFTDBPATH) = /DB2/trip`  
`DFTDBPATH` is the value that you need for the environment parameter DB2PATH.
5. The first time that you set up Db2 for exit, log in as Db2 OS user, and create the directory by entering one of these commands.
  - 64-bit environment: - `mkdir $DB2_PATH/sqllib/security64/plugin/commexit`
  - 32-bit environment: - `mkdir $DB2_PATH/sqllib/security/plugin/commexit`
6. As Db2 OS user, run the command: `ln -fs /usr/lib64/libguard_db2_exit_64.so $DB2_PATH/sqllib/security64/plugin/commexit/libguard_db2_exit_64.so`.  
 This allows Db2 to use the version-independent symbolic link that was created during S-TAP installation.
7. As `root` user, add the Db2 OS user to the `Guardium` group.  
 The `Guardium` group is created during S-TAP installation. This requirement increases the security of shared memory regions that are created by the S-TAP.
  - a. If Db2 user is 'trip', verify whether 'trip' is already authorized. Use `guardctl` under the A-TAP folder, as user `root`.

- ```
# /opt/IBM/guardium/module/modules/ATAP/current/files/bin/guardctl is-user-authorized trip
User 'trip' is authorized.
```
- b. If the user trip is not authorized, authorize it now:
- ```
/opt/IBM/guardium/module/modules/ATAP/current/files/bin/guardctl authorize-user trip
```
8. Enable Db2 Exit in Db2 (so it sends the database activity to the S-TAP).
- Log in as Db2 OS user and use the Db2 CLP commands to enable:  
`db2 UPDATE DBM CFG USING COMM_EXIT_LIST libguard_db2_exit_64`
  - Verify whether DB2\_Exit is successfully enabled by entering,  
`db2 get database manager configuration`  
If successful, the output includes,  
`Communication buffer exit library list (COMM_EXIT_LIST) = libguard_db2_exit_64`
9. Restart the Db2 database with the commands:
- ```
db2stop force
db2start
```
10. Set up Zone or WPARs,
- In the secondary Zone or WPAR, install the same version of S-TAP that is already installed in global, with K-TAP disabled.
 - On Zone or WPARs, add the DB2_EXIT IE in the guard_tap.ini or configure by using GUI.
 - If discovery automatically created any inspection engines, delete them.

Related tasks

- [Linux-UNIX: Upgrading S-TAP with databases that use an exit library](#)

Linux-UNIX: Configuring Informix Exit

The Informix exit module enables S-TAP to monitor any Informix database activities, whether encrypted or not and whether local or remote. It does not require A-TAP or K-TAP.

About this task

Informix Exit embeds a Guardium® library into the Informix database and communicates with the S-TAP via a Guardium shared library.

By default, Guardium supports up to 10 total Exit inspection engines (combined total of all Exit types). If you use more than one type of Exit, the combined maximum is 10. For more information, see the [exit_libs_num_threads](#) parameter in [Linux-UNIX: General parameters](#).

Informix Exit shared libraries are part of the Guardium Unix S-TAP installation. S-TAP includes 64-bit Exit libraries for 64-bit OS version and 32-bit Exit libraries for 32-bit OS version.

- `libguard_informix_exit_64.so`
- `libguard_informix_exit_32.so` (available for RHEL6 on the i686 CPU only)

When you install the S-TAP, it copies libraries in the standard library paths, and creates links, for example:

- It copies libraries in the standard library paths:
 - Shell Installation: <guardium_installation_directory>/guard_stap
 - GIM Installation: < guardium_installation_directory>/modules/STAP/current/files
- It creates links, for example:
 - `/usr/lib64/libguard_informix_exit_64.so -> libguard_informix_exit_64.so.<release number>`
 - `/usr/lib/libguard_informix_exit_32.so -> libguard_informix_exit_32.so.<release number>`

The digits after `.so`, reflect the release number. These digits were introduced in V10.6. (In previous releases, Lib files do not include release numbers.)
[Guardium support matrix](#) details exactly what can be monitored by Informix Exit.

If there is no other database to monitor then K-TAP is not required. Set `ktap_installed=0` in `guard_tap.ini`, or with GIM: set `ktap_enabled` to no. You can upgrade the Linux OS and the S-TAP without being concerned about K-TAP module compatibility. However, if there is another database that needs monitoring by S-TAP, then K-TAP is required. You must ensure that a compatible K-TAP module is available when you upgrade your Linux version.

When upgrading S-TAP from **v10.6.0.0 and higher**, database restart is not required. You can upgrade S-TAP while the database is running. The EXIT library from previous version is used until you restart the database, When you restart the database, it starts using the updated exit library. If there are any issues addressed in the new library that you are waiting for, you must restart the database.

Procedure

- Install and start up the S-TAP agent on the database server and configure an inspection engine for the informix exit protocol. See [Linux-UNIX: Installing, upgrading and uninstalling S-TAP agents](#) and [Linux-UNIX: Inspection engine parameters](#).
- Log in as user `informix` to the database and locate its instance name (INFORMIXSERVER) and its installation directory (INFORMIXDIR) by running these Unix commands:
`$ echo $INFORMIXSERVER
INFORMIXSERVER=test117
$ echo $INFORMIXDIR
INFORMIXDIR=/home/informix`

3. As user `root`, make sure the user `informix` is in the `guardium` group. If the user is not in the group `guardium`, use the `guardctl` utility to add the user to the group, for example:
`/usr/local/guardium/bin/guardctl authorize-user informix`
or with UNIX (AIX only):
`# chgroup users=informix guardium`
4. Copy `libguard_informix_exit` to the system standard library PATH (`/usr/lib64` or `/usr/lib`).
5. As user `informix`, create a link to the `informix_exit` library by running the command:
`ln -fs /usr/lib64/libguard_informix_exit_64.so $INFORMIXDIR/lib/libguard_informix_exit_64.so`
This allows `Informix` to use the version-independent symbolic link that was created during S-TAP installation.
6. To enable `informix_exit` monitoring you must start the `ifxguard` process. To start this process for first time run this command as user `informix`:
`ifxguard -p $INFORMIXDIR/lib/libguard_informix_exit_64.so -l $INFORMIXDIR/tmp/ifxguard.msg.txt`
After the `ifxguard` process starts, it automatically creates two files: one for configuration and one for messaging. The configuration file is created under `$INFORMIXDIR/etc/ifxguard.$INFORMIXSERVER` with these lines:
`NAME in2rh5u7_guard`
`LOGFILE /home/informix12/tmp/ifxguard.msg.txt`
`WORKERS 4`
`LIBPATH /home/informix12/lib/libguard_informix_exit_64.so`
7. Set up Zones/WPARs.
 - a. In the secondary Zone or WPAR, install same version of S-TAP that is already installed in global, with K-TAP disabled.
 - b. On Zone or WPARs, add Db2 EXIT IE in the `guard_tap.ini` or configure using GUI.
 - c. If discovery automatically created any inspection engines, delete them.
8. To restart the process in case the exit was reconfigured, the process hangs, or is not responding:
 - a. Disable `ifxguard`, as user `informix`, run the command: `ifxguard -k`
The output prints: `ifxguard in2rh5u7_guard successfully shut down`
 - b. To restart `ifxguard` after successful setup, as user `informix`, run the command `ifxguard`.
The output prints: `ifxguard set instance name in2rh5u7_guard Starting ifxguard in2rh5u7_guard ...`
check log file: `/home/informix12/tmp/ifxguard.msg.txt`
9. Restart the S-TAP.

Related tasks

- [Linux-UNIX: Upgrading S-TAP with databases that use an exit library](#)

Linux-UNIX: Configuring Teradata exit

The Teradata exit module enables S-TAP to monitor any Teradata database activities, whether encrypted or not and whether local or remote. It does not require A-TAP or K-TAP.

About this task

Teradata Exit embeds a Guardium® library into the Teradata database and communicates with the S-TAP through a Guardium shared library.

By default, Guardium supports up to 10 total Exit inspection engines (combined total of all Exit types). If you use more than one type of Exit, the combined maximum is 10. For more information, see the `exit_libs_num_threads` parameter in [Linux-UNIX: General parameters](#).

Teradata Exit shared libraries are part of the Guardium UNIX S-TAP installation. The S-TAP includes 64-bit Exit libraries for 64-bit OS version and 32-bit Exit libraries for 32-bit OS version:

- `libguard_teradata_exit_64.so`
- `libguard_teradata_exit_32.so` (available for RHEL6 on the i686 CPU only)

When you install the S-TAP:

- It copies libraries in the standard library paths:
 - Shell and RPM installation: <guardium_installation_directory>/guard_stap
 - GIM installation: <guardium_installation_directory>/modules/STAP/current/files
- It creates links, for example:
 - `/usr/lib64/libguard_teradata_exit_64.so -> libguard_teradata_exit_64.so.<release number>`
 - `/usr/lib/libguard_teradata_exit_32.so -> libguard_teradata_exit_32.so.<release number>`

The digits after `.so` reflect the release number. These digits were introduced in V10.6. (In previous releases, Lib files do not include release numbers.) [Guardium support matrix](#) details exactly what can be monitored by Teradata Exit.

Teradata configuration

The `gtwcontrol` option `-u SendConnectRespNoSecurity` specifies whether the gateway sends connection responses encrypted or cleartext. Valid values are:

- YES: The logon response is in cleartext (unencrypted plain text).
- NO: The logon response is encrypted. This is the default setting.

Set this parameter to Yes to capture DB User (-u YES). (When set to No, the connection response is encrypted before it gets to the `gtwgateway`, the process that loads the Guardium Exit library, and therefore cannot be passed unencrypted to Guardium.)

For more information, see [Teradata documentation](#).

K-TAP considerations

If there is no other database to monitor, then K-TAP is not required. Set `ktap_installed=0` in `guard_tap.ini`, or with GIM: set `ktap_enabled` to no. You can upgrade the Linux® OS and the S-TAP without being concerned about K-TAP module compatibility. However, if there is another database that needs monitoring by S-TAP, and K-TAP is required you must ensure that a compatible K-TAP module is available when you upgrade your Linux version.

Upgrade

When you upgrade S-TAP from **v10.6.0.0 and higher**, database restart is not required. You can upgrade S-TAP while the database is running. The Exit library from the previous version is used until you restart the database. When you restart the database, it starts using the updated exit library. If there are any issues that are addressed in the new library that you are waiting for, this is only resolved when you restart the database.

Procedure

1. Install and start the S-TAP agent on the database server and configure an inspection engine for the teradata_exit protocol. See [Linux-UNIX: Before you start installing S-TAP](#) and [Linux-UNIX: Inspection engine parameters](#). Use these parameters and values:

| GUI | guard_tap.ini | GUI Value / guard_tap.ini value |
|----------------|----------------|---|
| Protocol | db_Type | Teradata Exit / TRD_EXIT |
| ClientIP/Mask | networks | 0.0.0.0/0 / 0.0.0.0/0.0.0.0 |
| DB Install Dir | db_install_dir | Home directory of the user that runs the main Teradata process (pdemain), (using the following command <echo \$HOME>) |
| Process Name | db_exec_file | Full path to the main Teradat process (pdemain) |
| DB User | db_user | NULL (not relevant for Teradata exit) |

A typical DB section in the guard_tap.ini file for the inspection engine is:

```
[DB_0]
connect_to_ip=127.0.0.1
db_exec_file=/opt/teradata/tdat/tgtw/16.20.07.01/bin/pdemain
db_install_dir=/root
db_type=TRD_EXIT
db_user=NULL
encryption=0
db_version=9
intercept_types=NULL
load_balanced=1
port_range_end=0
port_range_start=0
priority_count=20
real_db_port=NULL
tap_identifier=TRD_EXIT_dbatera1620 (0,0,DB_0)
unix_domain_socket_marker=NULL
networks=0.0.0.0/0.0.0.0
exclude_networks=
```

When you are defining the inspection engine with the GUI, it looks like:

When the inspection engine is configured, it look like:

| Protocol | Port Range | TEE Listen Port-Real Port | | |
|---------------|------------|---------------------------|---------|--|
| Teradata Exit | 0-0 | | | |
| Ip | Mask | Connect To Ip | DB User | |
| 0.0.0.0 | 0 | 127.0.0.1 | NULL | |

2. As user root enable teradata exit in the database, while the database is running, by entering:

```
/usr/tgtw/bin/gtwcontrol --monitorlib load=yes
```

3. Stop the Teradata service:

a. Enter:

```
/etc/init.d/tpa stop
/etc/init.d/tgtw stop
```

b. Check that the Teradata database is stopped with your Teradata Administrator, or with the UNIX command:

```
pdestate -a
```

The response should be:

PDE state: DOWN/HARDSTOP

4. Authorize the required users:

a. As user **root**, verify that the users **teradata**, **tdatuser**, and **root** are in the **guardium** group. If any of the users are not in the group **guardium**, use the **guardctl** utility to add the user to the group. (The **teradata** and **tdatuser** users are the primary operating system-native users used in running Teradata DBS/PDE where they are created during Teradata Database installation process. **root** is the user of pdmain process.) For example:

- For shell installation:

```
<guardium_installation_directory>/guard_stap/guardctl authorize-user teradata  
<guardium_installation_directory>/guard_stap/guardctl authorize-user tdatuser
```

- For GIM installation:

```
<guardium_installation_directory>/ATAP/current/files/bin/guardctl authorize-user teradata  
<guardium_installation_directory>/ATAP/current/files/bin/guardctl authorize-user tdatuser
```

b. Confirm that the user is authorized with the option **is-user-authorized** in the **guardctl** command.

- For shell S-TAP installation:

```
<guardium_installation_directory>/guard_stap/guardctl is-user-authorized teradata  
<guardium_installation_directory>/guard_stap/guardctl is-user-authorized tdatuser  
<guardium_installation_directory>/guard_stap/guardctl is-user-authorized root
```

- For GIM S-TAP installation:

```
<guardium_installation_directory>/ATAP/current/files/bin/guardctl is-user-authorized teradata  
<guardium_installation_directory>/ATAP/current/files/bin/guardctl is-user-authorized tdatuser  
<guardium_installation_directory>/ATAP/current/files/bin/guardctl is-user-authorized root
```

5. As user **root**, create the directory **<teradata_install_directory>/tdat/tgtw/site** by running:

```
mkdir <teradata_install_directory>/tdat/tgtw/site
```

6. Set the permissions and the ownership for the directory: site.

- a. Enter:

```
chown -R teradata:tdtrusted <teradata_install_directory>/tdat/tgtw/site  
chmod -R 755 <teradata_install_directory>/tdat/tgtw/site
```

Note: In some cases permissions for **root** **root** also work.

- b. Confirm that the permissions are set correctly. For example:

```
db-teradata1610:~ #  
db-teradata1610:~ # ls -la /opt/teradata/tdat/tgtw/  
total 16  
drwxr-xr-x 4 root      root      4096 Jan 27 22:08 .  
drwxr-xr-x 8 teradata  tdtrusted 4096 Dec  7  2017 ..  
dr-xr-xr-x 6 teradata  tdtrusted 4096 Oct 27  2017 16.10.00.00  
drwxr-xr-x 2 teradata  tdtrusted 4096 Jan 27 22:08 site  
db-teradata1610:~ #
```

7. Start the Teradata service:

- a. Enter:

```
/etc/init.d/tpa start  
/etc/init.d/tgtw start
```

- b. Verify that the Teradata database is started with your Teradata Administrator, or with the UNIX command:

```
pdestate -a
```

The response should be:

```
PDE state is RUN/STARTED.  
DBS state is 5: Logons are enabled - The system is quiescent
```

8. Link the Teradata Exit library to the **libtgtwmonitoring.so**.

- a. As Teradara OS user, create the link for the full path of the Teradata Exit library from the standard system library path, either **/usr/lib** or **/usr/lib64**, depending on the OS version of your database server. This allows Teradata to use the version-independent symbolic link that was created during S-TAP installation.

```
ln -fs <standard_system_library_path>/libguard_teradata_exit_64.so  
<teradata_install_directory>/tdat/tgtw/site/libtgtwmonitoring.so
```

- b. Verify that the link is created, for example:

```
db-teradata1610:~ # ls -lrt /opt/teradata/tdat/tgtw/site/  
total 0  
lrwxrwxrwx 1 teradata  tdtrusted 39 Jan 27 22:08 libtgtwmonitoring.so -> /usr/lib64/libguard_teradata_exit_64  
.so
```

9. Confirm that the Teradata Exit library is loaded into the database by verifying The Monitoring Library: **load=yes** in response to the command:

```
/usr/tgtw/bin/gtwcontrol -d
```

```
db-teradata1610:~ # /usr/tgtw/bin/gtwcontrol -d
gtwcontrol: gtwversion 16.10.00.00
gdo version: 6, created on Mon Jan 28 17:11:31 2019

systemname: db-teradata1610
number of host groups: 1, number of gateway vprocs 1
max logfile size: 5000000
event trace cnt: 500
gtwglobal logon name: DBC
Send DBS error to client: no
Enable Channel Binding Support: no
TDGSS Library Version.....: 16.10.0.0
hgid: 1
    assign vprocid: 22528
    assigntrace: no
    logons enabled: yes
    session timeout in minutes: 20
    connection timeout in seconds: 60
    keepalive timeout in minutes: 10
    max sessions per gateway: 600
    iothread check frequency in minutes: 10
    max io threads per type (msg/net): 50
    initial io threads per type (msg/net): 25
    allow gateway testing enabled: no
    External Authentication: on
    Append Domain Name: no
    Reserved for Backdown: 0
    Require Confidentiality: yes
    Send Connect Response in cleartext: no
    Connection trace: no
    Local PE Preferred Percent: 0%
    TCP Socket SND/RCV Buffer Size: default (auto-tune)
    The Monitoring Library: load=yes,copy=no,trace=yes
    Audit Network Security: no
vproc id: 22528 status: Online
```

For example: db-teradata1610:~ #

- [Linux-UNIX: Disabling Teradata exit](#)

Follow this procedure to disable the Teradata exit library.

Related tasks

- [Linux-UNIX: Upgrading S-TAP with databases that use an exit library](#)

Related reference

- [Linux-UNIX: Inspection engine parameters](#)

Linux-UNIX: Disabling Teradata exit

Follow this procedure to disable the Teradata exit library.

Procedure

1. Verify that the "gtwgateway" process is running. Check that the Teradata database is running with your Teradata Administrator, or by using the UNIX command:

```
pdestate -a
```

The response should be:

```
PDE state is RUN/STARTED.
DBS state is 5: Logons are enabled - The system is quiescent
```

2. As root, unload the Teradata Exit library by entering:

```
/usr/tgtw/bin/gtwcontrol --monitorlib load=no
```

3. Stop the Teradata database:
 - a. Stop the Teradata service:

```
/etc/init.d/tpa stop  
/etc/init.d/tgtw stop
```

b. Verify that the Teradata database is stopped with your Teradata Administrator, or by using the UNIX command:

```
pdestate -a
```

The response should be:

```
PDE state: DOWN/HARDSTOP
```

4. If you are never going to enable the library again, delete the directory site by entering:

```
rm -f <teradata_install_directory>/tdat/tgtw/site
```

Linux-UNIX: Hadoop configuration

This topic introduces fundamental concepts and processes for monitoring Hadoop data with Guardium.

Capacity planning

The following sizing guidelines assume an average volume of audited traffic. Higher volumes of audited traffic may require additional resources.

- 10 management or server nodes per collector
- 20 or more data nodes per collector
- Possibly additional nodes per collector if physical appliances are used

It is also possible to size by the Processor Value Unit (PVU) of the nodes, but this may result in over-sizing if auditing low volumes of traffic. The capacity sizing guideline is 4000 PVU per collector.

There are a few options for integrating with Hadoop. The Ranger HDFS integration supports newer versions of Hortonworks and Cloudera (CDP 7.x). Use this integration when possible. Otherwise, choose your integration according to your cluster version. All integrations support SSL.

- [Linux-UNIX: Hadoop integration with Ranger HDFS for Hortonworks and Cloudera 7](#)

Hadoop services load a Ranger Audit Plugin. The Ranger Audit Plugin applies policies from the Ranger Policy Server. If an operation is covered by one of those policies and audit logging is enabled for the policy, the audit is logged to the Ranger Audit Server. The Ranger Audit Server can be configured to log audits to directories in HDFS. The S-TAP can consume Ranger audits from HDFS by connecting to the HDFS namenode, and reading Ranger audits for the services from the configured audit directory. S-TAP reads audits of each configured service from the oldest to the newest. This configuration uses the Cloudera Data Platform 7.x and Hortonworks 2.3 - 3.1 with Ranger HDFS.

- [Linux-UNIX: Hadoop integration with Cloudera Navigator](#)

Learn how to integrate Hadoop with Cloudera Navigator 5.8 - 6.3.x, Cloudera's native data governance solution.

- [Linux-UNIX: Hadoop integration using Hortonworks and Apache Ranger](#)

Apache Ranger, included with the Hortonworks Data Platform 2.3-2.6, offers fine-grained access control and auditing over Hadoop components such as Solr, Storm, Hive, HBASE, and HDFS by using policies.

Linux-UNIX: Hadoop integration with Ranger HDFS for Hortonworks and Cloudera 7

Hadoop services load a Ranger Audit Plugin. The Ranger Audit Plugin applies policies from the Ranger Policy Server. If an operation is covered by one of those policies and audit logging is enabled for the policy, the audit is logged to the Ranger Audit Server. The Ranger Audit Server can be configured to log audits to directories in HDFS. The S-TAP can consume Ranger audits from HDFS by connecting to the HDFS namenode, and reading Ranger audits for the services from the configured audit directory. S-TAP reads audits of each configured service from the oldest to the newest. This configuration uses the Cloudera Data Platform 7.x and Hortonworks 2.3 - 3.1 with Ranger HDFS.



Supported functions with Ranger HDFS for Hortonworks and Cloudera 7

You can use Ranger HDFS for Hortonworks and Cloudera 7 with the following functions:

- Audit SSL-encrypted activity
- Audit Kerberos authenticated traffic - By using Ranger integration, you do not need to propagate keytabs for Guardium.
- Audit Hive, HBASE, HDFS - HBASE deployment is simpler with Ranger, you do not need to deploy S-TAPs on data nodes.
- Audit SOLR
- Audit Kafka
- Audit Storm
- Audit Impala
- 12.1 and later Audit Atlas
- Audit exceptions - Ranger catches only "access denied" exceptions.

Limitations

Ranger integration supports the following policy rule actions:

- Alert daily
 - Alert only
 - Alert per match
 - Alert per time granularity
 - Log full details
 - Log full details with replaced values
 - Log masked details
 - Log only
 - No parse
 - Quick parse
 - Quick parse no fields
 - Record values separately
 - Skip logging
- [Linux-UNIX: Configuring S-TAPs: Ranger HDFS for Hortonworks and Cloudera 7](#)
Learn how to configure the S-TAP for Ranger HDFS integration.
- [Linux-UNIX: Upgrading and uninstalling S-TAPs: Ranger HDFS for Hortonworks and Cloudera 7](#)
You can upgrade or uninstall the S-TAP using the standard method for your installation type (e.g. shell, GIM, package).
- [Linux-UNIX: Ranger HDFS for Hortonworks and Cloudera 7 FAQs](#)
Find answers to some basic issues with Ranger HDFS integration.

Linux-UNIX: Configuring S-TAPs: Ranger HDFS for Hortonworks and Cloudera 7

Learn how to configure the S-TAP for Ranger HDFS integration.

Before you begin

Verify the following before you start:

- A functional Hortonworks cluster with [Ranger installed](#) and properly configured or a Cloudera Data Platform 7.x cluster with Ranger installed and configured. Ranger should be configured with policies to log all desired operations. Ranger should be configured to log audits to HDFS.
- If HDFS uses Kerberos, you need to specify the path to a keytab and a corresponding principal (ranger_hdfs_user).
- S-TAP is installed on a cluster node that has the proper HDFS libraries.
- The user with which S-TAP connects to HDFS must have the necessary permissions to read the files in the Ranger audit directories.

Procedure

1. Install the S-TAP or S-TAPs using the standard procedure for the chosen installer (GIM, shell, or RPM).
2. Browse to [Manage](#) > [Module Installation](#) > [Set up by Client](#), select the S-TAP or S-TAPs that are and set **STAP_RANGER_HDFS_READER_ENABLED=1**. (You can also directly modify the parameter **ranger_hdfs_reader_enabled** in the **guard_tap.ini** and restart the S-TAPs.) This step ensures that only the relevant S-TAPs display in the GUI.
3. Browse to [Setup](#) > [Tools and Views](#) > [Hadoop Monitoring](#) and click  in the Add cluster information tile.
4. Select Ranger HDFS from the Hadoop distribution drop-down menu.
5. From the Host name/IP drop-down list, select the Ambari server where the S-TAP is installed.
6. Configure the following parameters.

Table 1. Parameters for HDFS integration

| GUI | Default | Description |
|---------------------------|---------|---|
| HDFS audit directories | NULL | Comma-separated list of directories where Ranger logs the service audits. Include one directory that contains the daily log directories, for each service you want to monitor. Usually the paths are located under /ranger/audit.

Example service directories for CDP 7: /ranger/audit/hive/hiveServer2,/ranger/audit/kafka/kafka,/ranger/audit/hbase/hbaseMaster,/ranger/audit/hbase/hbaseRegional,/ranger/audit/atlas/atlas,/ranger/audit/hdfs/hdfs

Example service directories for HW 3: /ranger/audit/hbaseMaster,/ranger/audit/hbaseRegional,/ranger/audit/hdfs,/ranger/audit/hiveServer2,/ranger/audit/kafka,/ranger/audit/solr,/ranger/audit/storm |
| HDFS lib location | NULL | Locate libhdfs.so provided by Hadoop cluster (for example, /usr/hdp/3.1.0.141-1/usr/lib/libhdfs.so) and set ranger_hdfs_lib_location to the directory that contains libhdfs.so (for example, /usr/hdp/3.1.0.141-1/usr/lib). |
| HDFS name node | NULL | IP or hostname of the HDFS NameNode. |
| HDFS poll (milliseconds) | 100 | Time interval, in milliseconds, the S-TAP waits between checking for new Ranger audits in HDFS. |
| HDFS port | 8020 | The HDFS NameNode port the S-TAP connects to. |
| HDFS user | NULL | The user with which S-TAP connects to HDFS. If the HDFS setup is using Kerberos, set the parameter to the Kerberos principal. |
| LD library path | NULL | Locate libjvm.so (for example, /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.191.b12-1.el7_6.x86_64/jre/lib/amd64/server/libjvm.so) and set ld_library_paths to the directory that contains libjvm.so (for example, /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.191.b12-1.el7_6.x86_64/jre/lib/amd64/server). |
| HDFS audit history length | 30 | The length of the audit history. <ul style="list-style-type: none"> • A positive value is the history length in days, maximum = 2147483647. The default is 30 (days). • A negative value is the history length in hours, maximum = -2147483648. • 0 - The S-TAP reads audits from the first audit that was written into the Ranger audit logs. |
| Use Kerberos | | Check to use Kerberos authentication. |
| Principal | | Required for Kerberos. The value of Ranger HDFS user. |

| GUI | Default | Description |
|-------------|---------|---|
| HDFS keytab | NULL | Required for Kerberos. Location of the Kerberos keytab that contains the principal used to connect to HDFS. |

7. Click Save.

Related reference

- [Linux-UNIX: Hadoop parameters](#)
- [Hadoop monitoring APIs](#)

Linux-UNIX: Upgrading and uninstalling S-TAPs: Ranger HDFS for Hortonworks and Cloudera 7

You can upgrade or uninstall the S-TAP using the standard method for your installation type (e.g. shell, GIM, package).

There are no special steps required for upgrading or uninstalling S-TAPs that are used in a Ranger HDFS integration.

Linux-UNIX: Ranger HDFS for Hortonworks and Cloudera 7 FAQs

Find answers to some basic issues with Ranger HDFS integration.

HDFS audits are not being processed and the following message is seen in the STAP logs:

```
2020.04.22 12:55:35 ranger_hdfs_integration/guard_hdfs.cc(78) HDFS: cannot load libhdfs, no path provided
Verify that ranger_hdfs_lib_location is set to the directory containing libhdfs.so on the server hosting S-TAP.
```

HDFS audits are not being processed and the following message is seen in the STAP logs:

```
2020.04.22 12:57:52 ranger_hdfs_integration/guard_hdfs.cc(111) HDFS: unable to open /tmp/libhdfs.so, error: /tmp/libhdfs.so: cannot open shared object file: No such file or directory
```

Verify that ranger_hdfs_lib_location is set to the directory containing libhdfs.so on the server hosting S-TAP.

HDFS audits are not being processed and the following message is seen in the STAP logs:

```
2020.04.22 12:59:20 ranger_hdfs_integration/guard_hdfs.cc(111) HDFS: unable to open /usr/hdp/3.1.0.0-78/usr/lib/libhdfs.so, error: libjvm.so: cannot open shared object file: No such file or directory
```

Verify that ld_library_paths is set to the directory containing libjvm.so on the server hosting S-TAP.

HDFS audits are not being processed and the following message is seen in the STAP logs:

```
hdfsExists: invokeMethod((Lorg/apache/hadoop/fs/Path;)Z) error: ConnectException: Connection refusedjava.net.ConnectException: Call From <STAP_HOSTNAME>/<STAP_IP> to <NN_HOSTNAME>/<PORT> failed on connection exception: java.net.ConnectException: Connection refused; For more details see: http://wiki.apache.org/hadoop/ConnectionRefused
For more details see: http://wiki.apache.org/hadoop/ConnectionRefused.
```

Verify that ranger_hdfs_namenode and ranger_hdfs_port are correct. Also, ensure that the HDFS NameNode is up and running.

HDFS audits are not being processed and the following message is seen in the STAP logs:

```
hdfsBuilderConnect(forceNewInstance=0, nn=hw3-cl1-01.swg.usma.ibm.com, port=8020,
kerbTicketCachePath=/usr/local/guardium/guard_stap/hdfs_reader_ticket, userName=foobar) error: LoginException: Unable to obtain password from user org.apache.hadoop.security.KerberosAuthException: failure to login: for principal: foobar using ticket cache file: /usr/local/guardium/guard_stap/hdfs_reader_ticket javax.security.auth.login.LoginException: Unable to obtain password from user
```

There is an issue with the keytab or principal S-TAP is configured to use. Verify that the ranger_hdfs_keytab and ranger_hdfs_user are correct for the environment.

HDFS audits are not being processed and a message similar to the following is seen in the STAP logs::

```
CannotObtainBlockLengthException: Cannot obtain block length for LocatedBlock {BP-475011667-9.32.164.237-1546906377615;blk_1074457421_717409; getBlockSize()=428; corrupt=false; offset=0; locs=[DataNodeInfoWithStorage[9.32.164.137:1019,DS-39fe5b73-f666-4285-bd50-805b4acc9250,DISK], DataNodeInfoWithStorage[9.32.164.148:1019,DS-fd105fa3-aa8e-44f5-a878-7d409ea6d24f,DISK]]}
```

ON an HDFS client for the HDFS cluster, enter the command **hdfs debug recoverLease** for the ranger audit log file whose name appears just before the **CannotObtainBlockLengthException** message, using the syntax:

```
hdfs debug recoverLease -path <path to audit file> -retries <number of times to try to recover the lease on the HDFS file>
```

For example:

```
hdfs debug recoverLease -path /ranger/audit/solr/20200623/solr_ranger_audit_hw3-cl1-02.log -retries 10
hdfs debug recoverLease -path /ranger/audit/storm/20200812/storm_ranger_audit_hw3-cl1-01.log -retries 10
```

For more information, see [Cannot obtain block length for LocatedBlock](#).

Linux-UNIX: Hadoop integration with Cloudera Navigator

Learn how to integrate Hadoop with Cloudera Navigator 5.8 - 6.3.x, Cloudera's native data governance solution.

Guardium provides the capability to subscribe to audit events when Cloudera Navigator is configured to publish audits to Kafka. Audited activity is sent to a Kafka cluster where the Guardium S-TAP consumes the events and sends them to the Guardium collector to be parsed and logged. The data is highly protected in the hardened Guardium system. All normal Guardium functions can be used, such as real-time alerting and integration with SIEM, reporting and workflow, and analytics.

Why integrate with Navigator? A key reason is the fact that many organizations are now using SSL encryption for their clients to access Hadoop data. By using this integration, events can be monitored even though the wire traffic is encrypted. Support for Kerberos and LDAP authentication is also easier with the Navigator integration since no special keytab configuration is required.

The Cloudera version that is referenced in this content is https://docs.cloudera.com/documentation/enterprise/6/6.3/topics/cn_iu_introduce_navigator.html

Guardium functions supported with Navigator

- Audit SSL-encrypted activity
- Audit Kerberos-authenticated traffic - With Navigator integration, you do not need to propagate keytabs for Guardium.
- Audit Hive, HBASE, HDFS, Impala
- Audit Solr
Note: For Navigator, only commands that are issued with **solrctl** are collected, not normal user activity.
- Audit Sentry
- Audit exceptions

Limitations and restrictions

- Guardium-based blocking does not support any Hadoop components with Cloudera Navigator integration.
- The supported policy rule actions are:
 - Alert per match
 - Log only
 - Skip logging
 - Alert daily
 - Alert only
 - Alert per time granularity
 - Log full details with replaced values
 - Log masked details
 - No parse
 - Record values separately
 - Quick parse
 - Quick parse no fields
- Capturing failed logins from Hue requires Cloudera Manager 5.8 or later.
- Access to “new projects and documents” from Hue are not captured by Navigator and thus are not captured by Guardium.
- In Hbase, Navigator access through Hue reports only the DB User of HBASE or HUE.
- In HBase, Navigator captures the Grant commands but not the user that is granted.
- When using Impala statements with Cloudera Navigator, statements across multiple lines are merged into a single-line statement. As a result, statements that use single-line comments (that is, comments that begin with two dashes [--]), can cause errors. To use comments with Impala statements, use one of the following techniques:
 - Use comments that begin with two dashes (--) only at the very end of the statements.
 - Wrap all comments in slash-asterisk format /* comment */. For example,

```
select * from user_table from all_users
/* comment appearing within the statement */
where user_age > 70 and user_location in ('TAIWAN', 'JAPAN');
```

Prerequisites

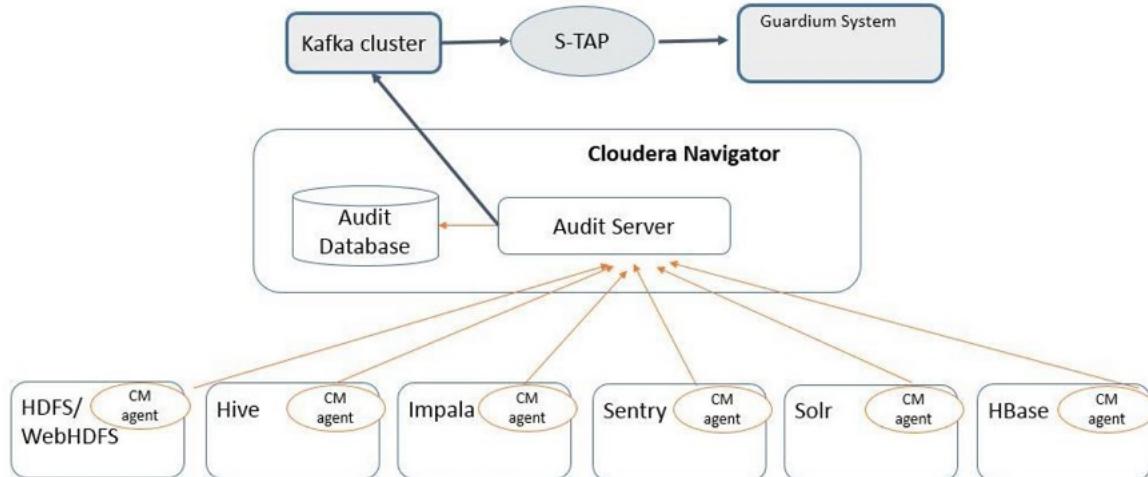
Guardium integration with Cloudera Navigator requires the following minimum software release levels:

- IBM Security Guardium and S-TAP at V10.1.2 or later.
- CDH 5.7, and Cloudera Manager 5.8, and the Kafka included with those versions.

Architecture and data flow

Instead of locating an S-TAP on the Hadoop servers, the Cloudera Manager agent sends audit events from the Hadoop component logs to the Navigator audit server. At that point, Navigator writes the audit events to its audit database. To integrate with Guardium, set up Navigator to publish. Guardium gathers the event records from Kafka.

Figure 1. S-TAP reads Navigator audit events off the Kafka cluster



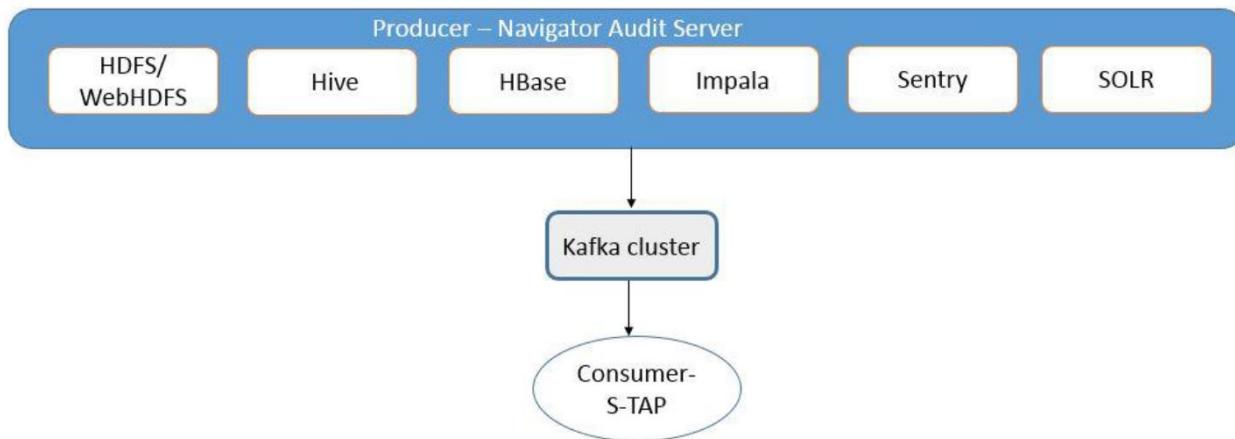
Configuration is flexible. You can install the S-TAP:

- On a node in the Hadoop cluster.
- On a separate server outside of the Hadoop cluster, if that server has network connectivity to the Kafka cluster and the Guardium appliance.

Configuring multiple STAPs for the same Kafka cluster and specifying the same kafka_group_name allows the Kafka cluster to balance the load of the topics and partitions over the S-TAPs.

In this configuration, Navigator produces the log events for each Hadoop component, and the S-TAP consumes those events. Using the Guardium user interface, you specify the message topic identifier that Navigator uses so that the Guardium S-TAP knows which events it is supposed to pick up.

Figure 2. Audit events are written to the Kafka cluster where S-TAP picks them up



Recommendation: Use a secure Kafka cluster to ensure that your audit events are protected.

A few words about Kafka. Apache Kafka is a distributed messaging system.

- A server in a Kafka cluster is a Broker.
- Message writers are called Producers.
- Message readers are called Consumers.
- A message category is called a Topic.

[Linux-UNIX: Planning the integration with Cloudera Navigator](#)

Integrating with Cloudera Navigator requires gathering some information from the administrators responsible for Cloudera and Kafka, as well as from the data security team responsible for Guardium. Gather the following information before you begin.

[Linux-UNIX: Preliminary configuration](#)

This section covers the preparatory configuration: the Navigator auditing component, verifying that TLS/SSL is configured correctly for Kafka, installing S-TAP on a server

[Linux-UNIX: Configure publication of Navigator audit events to Kafka](#)

The Navigator administrator or full administrator must do this task from Cloudera Manager.

[Linux-UNIX: Configuring the S-TAP for Cloudera](#)

Configure the S-TAP to establish communication between the Guardium system and Cloudera Navigator that uses a Kafka cluster.

[Linux-UNIX: Validate and troubleshoot the Cloudera configuration](#)

Check that the Cloudera configuration successfully captures traffic.

Related reference

- [Hadoop parameters](#)

Linux-UNIX: Planning the integration with Cloudera Navigator

Integrating with Cloudera Navigator requires gathering some information from the administrators responsible for Cloudera and Kafka, as well as from the data security team responsible for Guardium. Gather the following information before you begin.

- Host and ports for the Kafka bootstrap servers.
- Whether TLS and Kerberos are used in the Kafka cluster. See [2 in Linux-UNIX: Preliminary configuration](#).
- The host and port for the server where the S-TAP is installed. Verify that there is network connectivity between this server and both the Kafka cluster and the Guardium collector.
- The operating system and version used on the S-TAP host so you can download and install the correct S-TAP.
- The host for the Guardium system. This is required for installing and configuring the S-TAP.

Linux-UNIX: Preliminary configuration

This section covers the preparatory configuration: the Navigator auditing component, verifying that TLS/SSL is configured correctly for Kafka, installing S-TAP on a server

Procedure

1. Configure the Navigator auditing component.
 - If you do not already have Navigator configured to audit the supported services as normal, without Guardium, refer to Cloudera documentation for more information about setting that up. Be aware that you may need to specifically enable the configuration for each service, depending on the level of Cloudera that you have. Solr auditing is disabled by default. You must enable it following the instructions in the Cloudera documentation.

Figure 1. Enabling Solr audit in Cloudera Manager

| Category | Property | Value | Description |
|--------------------|-------------------------|---|---|
| ▼ Service-Wide | Enable Audit Collection | <input checked="" type="checkbox"/> Reset to the default value: false | Enable collection of audit events from the service's roles. |
| Advanced | | | |
| Cloudera Navigator | | | |
| Logs | | | |

- To get Impala traffic, you need to enable Impala Daemon auditing as described in the Cloudera documentation. Here's a screenshot from the Impala service configuration in Cloudera Manager that shows Impala audit event generation is enabled.

Figure 2. Enabling audit events for Impala in Cloudera Manager

| Property | Value | Description |
|--------------------------------------|---|--|
| Enable Impala Audit Event Generation | <input checked="" type="checkbox"/> Reset to the default value: false | Enables audit event generation by Impala daemons. The audit log file will be placed in the directory specified by 'Impala Daemon Audit Log Directory' parameter. |
| enable_audit_event_log | Impala audit log is set when Navigator audit collection is enabled. | |

2. Verify that TLS/SSL is configured correctly for Kafka.

The Kafka cluster you use for producing Cloudera audit events must not be configured with required SSL client authentication. In Cloudera Manager, go to Kafka Configuration > SSL client authentication and choose the none or requested radio button.

3. Install the S-TAP on the designated server inside or outside of the Hadoop cluster.

- Use the appropriate procedure for your system. See [Linux-UNIX: Installing, upgrading and uninstalling S-TAP agents](#).
- Verify connectivity between the S-TAP and the Guardium system. The S-TAP status should be green in the S-TAP Status Monitor page. Go to Manage > System View > S-TAP Status Monitor.

Linux-UNIX: Configure publication of Navigator audit events to Kafka

The Navigator administrator or full administrator must do this task from Cloudera Manager.

Procedure

- Go to Cluster > Cloudera Management Service > Cloudera Management Service
- Click the Configuration tab. From the left navigation menu choose the category Publishing.
- For Kafka Service, select the Kafka radio button. The default topic name for Navigator event publishing is NavigatorAuditEvents. You can change this, but if you do, be sure to change it also in the S-TAP configuration to be a matching name. See [Linux-UNIX: Configuring the S-TAP for Cloudera](#).

Linux-UNIX: Configuring the S-TAP for Cloudera

Configure the S-TAP to establish communication between the Guardium system and Cloudera Navigator that uses a Kafka cluster.

About this task

You can also configure the S-TAP directly in the guard_tap.ini file. Restart the S-TAP for the configuration to take effect.

Procedure

- Browse to Setup > Tool and Views > Hadoop Monitoring and then click the add icon (+) in the Add cluster information tile.
- Select Cloudera as the Hadoop distribution.
- Select an S-TAP that is connected to the Guardium system in the S-TAP host name drop-down list.
- Enter the Kafka details.
 - Group name. The name of the Kafka consumer group you want this S-TAP to be a part of.
 - Topic name for the Kafka cluster. Unless this setting was changed in the Kafka cluster configuration settings, use the default NavigatorAuditEvents. For more information about configuring the Kafka cluster, see the Cloudera documentation.
 - Bootstrap servers. One or more Kafka nodes to take the initial connection from the Guardium S-TAP. Both host name and port are required for each server. Any nodes that are leaders of a partition for the topic can handle consumer requests. For the initial connections, it's best to specify more than one server to provide a failover in case one of the bootstrap servers is down.
 - LD library path. Path to the directory that contains the guard_stap binary, indicating to the S-TAP about which libraries to load. (For example, /usr/local/guardium/guard_stap or /usr/local/modules/STAP/current.)
- If your Kafka cluster is configured with TLS, check Enable TLS.

Restriction: Guardium does not support Kafka clusters that are configured to require SSL client authentication.

 - SSL CA path. Required parameter for TLS. Path to a file that contains the certificate to verify the Kafka broker's certificate, in PEM format. You can have a file that contains multiple certificates in a single file.
- If the Kafka cluster requires Kerberos authentication, check Use Kerberos, and enter the Kerberos details.
 - Principal. The Kerberos principal name for the S-TAP. For example, guardium/FullyQualifiedDomainName@kerberosDomain

- Path to keytab file, the full path to the Kerberos keytab file on the S-TAP server. For example, /etc/krb.keytab. Verify that the keytab is owned by the S-TAP user and group, and is only readable by the user.
7. Click Save.
The NavigatorAuditEvents pop-up opens, showing that monitoring is enabled. If the S-TAP status is not green, investigate its status.

Related reference

- [Linux-UNIX: Hadoop parameters](#)

Linux-UNIX: Validate and troubleshoot the Cloudera configuration

Check that the Cloudera configuration successfully captures traffic.

Procedure

1. Go to the S-TAP Status Monitor page and verify that the S-TAP is still green. (Inspection engine verification is not supported for Hadoop sources, so that is always Unverified.)
2. Install a Guardium policy, or use the default policy, then run some simple HDFS or Hive commands on the Cloudera cluster and see if you can see the traffic in a report or, after a bit of time, in the investigation dashboard.
3. Troubleshooting: If you are not seeing traffic from Navigator, check the following:
 - In Cloudera Manager, verify that auditing is enabled for each service you want to monitor.
 - Is integration enabled? Check the S-TAP configuration to make sure that the kafka_reader_enabled=1.
 - Is the Kerberos principal and path correct?
 - Are the Kafka bootstrap servers up and running?
 - If TLS is checked in the GUI, verify that Kafka is setup for TLS, and vice versa. Also verify that TLS on the Kafka is not configured with client authentication required.
 - Double check your Guardium policy to make sure you are logging the traffic you expect to see from Navigator.
 - Check your report to see if you have defined it correctly. (Server type group, now -n days, and so on.)

Linux-UNIX: Hadoop integration using Hortonworks and Apache Ranger

Apache Ranger, included with the Hortonworks Data Platform 2.3-2.6, offers fine-grained access control and auditing over Hadoop components such as Solr, Storm, Hive, HBASE, and HDFS by using policies.

The audit data is written to both HDFS and Solr. Guardium can integrate with Ranger in two ways:

- For auditing, Guardium acts as another logger source for Ranger Auditing. Audited activity is sent to the Guardium collector where it is parsed and logged. After the data is in Guardium, it is highly protected in the hardened appliance. You can use all normal Guardium functions, such as real-time alerting and integration with SIEM, reporting and workflow, and analytics.
- For blocking, Guardium extends Ranger access control policies, by using what is known in Ranger as dynamic policies.

With Ranger integration, the data is decrypted before it is sent to the Guardium system for auditing. In addition to SSL support, Ranger integration that uses dynamic policies enables blocking support for more components than is supported by standard S-TAP.

Supported functions with Ranger integration

You can use Ranger integration with the following functions:

- Audit SSL-encrypted activity
- Audit Kerberos authenticated traffic - By using Ranger integration, you do not need to propagate keytabs for Guardium.
- Audit Hive, HBASE, HDFS - HBASE deployment is simpler with Ranger, you do not need to deploy S-TAPs on data nodes.
- Audit SOLR
- Audit Kafka
- Audit Storm
- Audit exceptions - Ranger catches only "access denied" exceptions.
- Blocking of Hive, HDFS, and HBASE with dynamic policies.

Limitations

Ranger integration supports the following policy rule actions:

- Alert daily
- Alert only
- Alert per match
- Alert per time granularity
- Log full details
- Log full details with replaced values
- Log masked details
- Log only
- No parse
- Quick parse
- Quick parse no fields
- Record values separately

- Skip logging
- [Linux-UNIX: Hortonworks Ranger architecture and data flow](#)
Learn how the monitoring and audit, and the blocking, are implemented.s
- [Linux-UNIX: Planning the integration with Hortonworks and Apache Ranger](#)
Complete and verify the tasks in this topic before configuring the integration.
- [Linux-UNIX: Hortonworks and Apache Ranger prerequisites](#)
Verify these prerequisites before starting your integration.
- [Linux-UNIX: FAQs Hortonworks Ranger configuration](#)
Read answers to the most asked questions about the Hortonworks Ranger configuration.
- [Linux-UNIX: Configure the solution for monitoring](#)
This section describes how to configure the solution for monitoring.

Related reference

- [Hadoop parameters](#)

Linux-UNIX: Hortonworks Ranger architecture and data flow

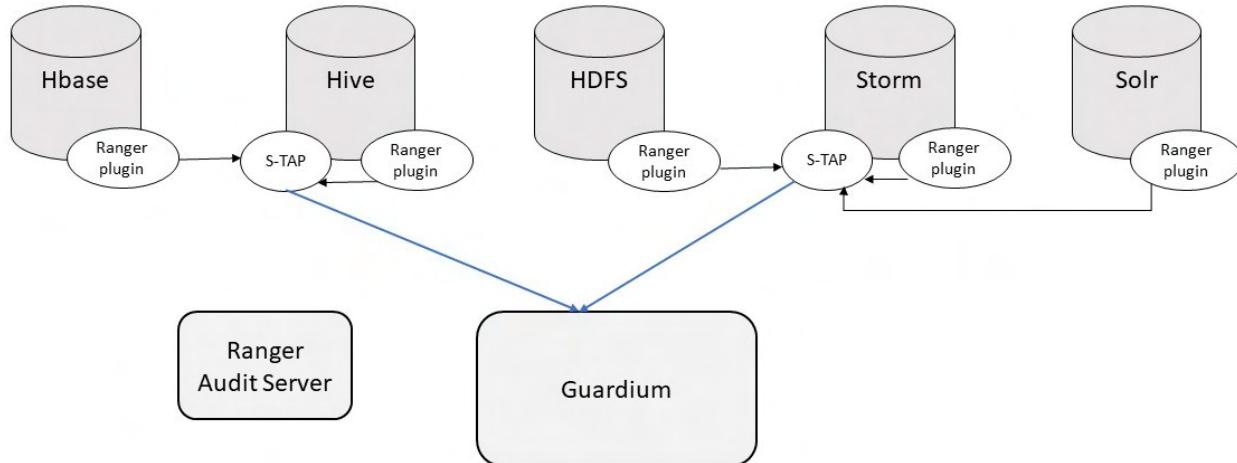
Learn how the monitoring and audit, and the blocking, are implemented.s

Monitor and Audit

The important difference with this architecture is that the S-TAP is not collecting audit data directly from the Hadoop component; instead the Ranger plugins write the audit messages to log4j, which forwards them to the S-TAP. The S-TAP then sends the messages to the Guardium collector for logging, alerting, reporting, and analytics.

The configuration is quite flexible in that you can install S-TAPs on more nodes. You can configure Ranger to send all component traffic to one S-TAP or you could specify, for example, that all HBase traffic goes to one S-TAP and Hive and HDFS goes to another.

Figure 1. Ranger plugin using log4j as an alternate logging source, forwarding audit data to Guardium



Blocking (Ranger Dynamic Policy integration)

Blocking is implemented by extending Ranger access control policies to honor blocking policy rules that are specified on the Guardium appliance. The actual implementation of blocking is performed as an access denial from Ranger. For more information about how blocking fits into the architecture and data flow and guidance for implementing blocking, see [IBM Security Monitoring and Blocking for Hortonworks Hadoop Using Apache Ranger Integration](#).

For blocking, you need an additional component called the Guardium plug-in for Ranger. This plug-in is called `guardium_evaluator.jar` and resides alongside the Ranger plugin on the Hadoop component nodes. You need this on the data/slave nodes as well if you want to block HBase.

S-TAPs required: You do not need any additional S-TAPs than what is already required for monitoring/auditing. It makes sense to use the same collector/S-TAP combinations for blocking as you do for auditing.

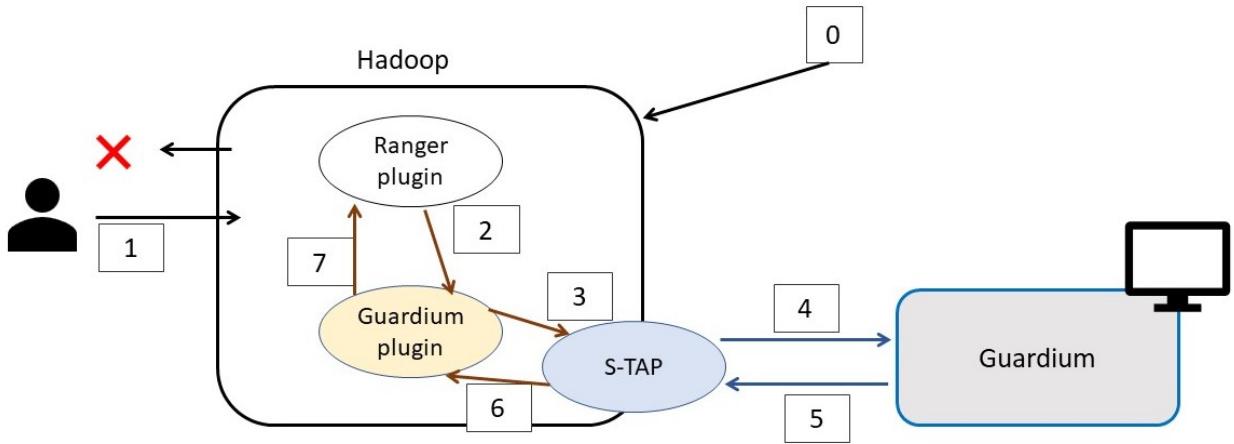
Prerequisite (**Step 0**): The administrator sets up filtering conditions on a Ranger policy based on resource, user or group or other conditions allowed by Ranger. For simplicity, let's call this the "watch" criteria. For example, the Ranger policy might specify Scott's activity against certain resources, because he's a privileged user. The policy also includes a condition to call the Guardium evaluator plugin. For more information about creating Ranger policies, see the Hortonworks documentation and Ranger tutorials.

The administrator sets up S-TAP to enable integration with the dynamic policies and the firewall. The S-TAP does not have to be directly co-located the Ranger or Guardium plugins.

On the Guardium appliance, install a policy that includes the rule action of S-GATE Terminate for inappropriate access to Hadoop. This rule could include additional criteria such as client IP address or other runtime information.

[Figure 2](#) illustrates the blocking flow, described by the following text.

Figure 2. Blocking flow with Guardium and Hortonworks Ranger



1. User tries to access a resource that meets the “watch” criteria.
2. Ranger plugin sends information about this access to the Guardium plugin.
3. Guardium plugin sends message to S-TAP.
4. S-TAP sends request to appliance about this access.
5. If Guardium blocking policy rule conditions are met, the Guardium appliance sends “block” response to S-TAP
6. S-TAP sends “block” to Guardium plugin
7. Guardium plugin tells Ranger not to match the original watching rule. This means that if there is no other Ranger policy that allows access to the resource, then access will not be allowed to the resource.

Linux-UNIX: Planning the integration with Hortonworks and Apache Ranger

Complete and verify the tasks in this topic before configuring the integration.

Topology of S-TAPs and collectors

Determine the required topology:

- Number of collectors needed
- Components monitored by each S-TAPs

Some customers prefer to have one S-TAP for each component. At a minimum, we recommend one S-TAP for HBase and one S-TAP for everything else.

Tip: An S-TAP is not required to sit on the same node as any particular component. It's possible--and even advisable if supporting Hadoop HA--to establish a dedicated Linux box for an S-TAP.

When configuring the number of connections for an S-TAP, use the following rule of thumb:

- HBase: one plus the number of region servers
- Everything else: one plus one for each component monitored

Attention:

- For blocking, verify access to all HBase region servers, since you will need to copy the Guardium plugin JAR file to each of these region servers.
- For configuring high availability failover scenarios, record the failover node IP addresses or host names.

High availability and failover

Hadoop uses secondary nodes for high availability to handle data requests should the primary node fail. There are several options for S-TAP deployment so that you can continue to collect audit data in a failover scenario.

Install the S-TAP and set it up on a system that is not part of the Hadoop cluster

This provides a simple configuration where, when the components fail over, the new node automatically uses the S-TAP as a remote logger. No changes are needed to any configurations or S-TAPs.

Hybrid approach (recommended)

Install an S-TAP for HDFS and Hive using `localhost` in the S-TAP host field, then use a separate system such as an edge node for HBase. This provides an alternative to installing S-TAPs on all nodes and region servers and is the recommended approach.

Install the S-TAP on the nodes in the cluster

In this model, you install an S-TAP on the primary and standby node for each component.

Using `localhost` in the S-TAP host field, install an S-TAP on every node in the cluster and every region server for HBASE. This is approach is not recommended.

Guardium load balancing

Guardium S-TAP and enterprise load balancing options are supported when Ranger integration is enabled.

Linux-UNIX: Hortonworks and Apache Ranger prerequisites

Verify these prerequisites before starting your integration.

- S-TAP and appliance are running Guardium V10.1 or later
- Hortonworks 2.3-3.1 with Ranger
- For Hive 3+, log4j libraries must be replaced by log4j 2.8 libraries for hiveserver2 in /usr/hdp/current/hive-server2/lib directory. The correct libraries are:
 - log4j-1.2-api-2.8.2.jar
 - log4j-api-2.8.2.jar
 - log4j-core-2.8.2.jar
 - log4j-slf4j-impl-2.8.2.jar
 - log4j-web-2.8.2.jar

You can download the libraries from <https://logging.apache.org/log4j/log4j-2.8/download.html>

- Solr Component is configured (mandatory Ranger component that enables display of user information in Guardium)
- Ambari and Ranger information. A significant portion of setup is done through Ambari, the Hadoop administrative interface. You need the following information:

Ambari

- A user ID and password who has privileges to update and save the *log4j* configuration, such as a Service Administrator account. For simplicity, refer to this as the admin account and password.
- Port and IP address or hostname.
- Cluster name.

Ranger

The details are only needed if configuring blocking. For more information about configuring blocking, see [IBM Security Monitoring and Blocking for Hortonworks Hadoop Using Apache Ranger Integration](#).

- A Service Administrator account that can update and save the *log4j* configuration.
- Port and IP address or hostname.

- These ports must be open (assuming use of default ports):

- For monitoring, open port 5555 between the node(s) that S-TAP is on and the Ranger server.
- For blocking, open port 5556 to allow communication between S-TAP and all nodes in the cluster that have the Guardium plugin.

Linux-UNIX: FAQs Hortonworks Ranger configuration

Read answers to the most asked questions about the Hortonworks Ranger configuration.

What Hadoop service components connect to the S-TAP?

https://docs.hortonworks.com/HDPDocuments/HDP2/HDP-2.6.4/bk_command-line-installation/content/installing_ranger_plugins.html lists where the Ranger plug-ins are installed for each Hadoop service. These plug-ins are what connect to the S-TAP.

Can multiple STAPs be configured per Hadoop service?

It depends. The Ranger plug-ins for the service connect to the S-TAP. If your HDFS service has only a single NameNode, there can be only one connection for that service. If there are multiple components with Ranger plug-ins (for example, HBASE, which has the Ranger plug-ins on the Master server, and on every Region server), multiple connections can be made. The main issue is that all components of the Hadoop service share one configuration. As a result, the remote host parameter of the Guardium® log4j logger is the same. One option is to put "localhost" as the host to log to and install an S-TAP on every node that has a Ranger plug-in for that service. Another option is to use DNS round robin to have each plug-in connect to a different S-TAP. Another option is to use configuration groups to specify different Guardium log4j logger remote hosts for the different Hadoop service components.

Why does the x service show up in reports for the y service?

Hadoop services often utilize each other for various functions. It is normal to see references to other Hadoop services in reports.

What is missing if the Ranger plug-in for x service is not configured?

All audits related to that service are not logged.

Can Ranger policies be configured in a way to filter audits to S-TAP while retaining audits in Ranger?

No. If actions match a Ranger policy and that policy has auditing enabled, the audit goes to all audit destinations.

Is an inspection engine needed for Hortonworks integration?

No. Inspection engines are not needed for Hadoop services that use the integration to send audits.

The Guardium UI is showing monitoring enabled, but the Ranger plug-ins are not installed yet. What is happening?

Guardium checks only that the Guardium log4j logger exists in the Hadoop service logging configuration. It does not check whether the Ranger plug-ins are installed, or if the Ranger repository and policies exist.

Linux-UNIX: Configure the solution for monitoring

This section describes how to configure the solution for monitoring.

1. [Linux-UNIX: Configure the Ranger plugins using Ambari](#)

Use this procedure to enable Ranger plug-ins for the Hadoop components you want to monitor. Refer to Hortonworks documentation for more details as needed or if you need to enable auditing on a non-Ambari cluster.

2. [Linux-UNIX: Configure Guardium and Ranger communication](#)

Learn how to establish communication between the Guardium system and Ranger.

3. [Linux-UNIX: Install and configure S-TAPs](#)

Install and configure S-TAPs for Ranger integration.

Linux-UNIX: Configure the Ranger plugins using Ambari

Use this procedure to enable Ranger plug-ins for the Hadoop components you want to monitor. Refer to Hortonworks documentation for more details as needed or if you need to enable auditing on a non-Ambari cluster.

Procedure

1. In Ambari, log in as the administrator. Go to Ranger > Configs > Ranger Plugin and enable the relevant Ranger plugins (HDFS, Hive, Kafka, HBase, Storm, Solr).
2. Create repositories for all the components to be audited.
3. Restart Ranger and the components.
4. Ensure Ranger auditing is turned on for each component's Ranger policies. By default, they are enabled, but you can verify in the Ranger console.

Next topic: [Linux-UNIX: Configure Guardium and Ranger communication](#)

Linux-UNIX: Configure Guardium and Ranger communication

Learn how to establish communication between the Guardium system and Ranger.

Before you begin

- If you are using SSL, add the certificate to the keystore with the CLI command **store certificate keystore trusted console**.

You can perform the equivalent procedure using the APIs [add_ranger_config](#) and [add_ranger_service](#).

Procedure

1. Go to Setup > Tools and Views > Hadoop Monitoring.
2. Click  in the Add cluster information section to begin defining a new configuration.
3. Select **Hortonworks** from the Hadoop distribution menu.
4. Host name/IP - Enter the host name or IP address of the Ambari server.
5. Port number - Enter the Ambari server port number.
If you leave this field blank, the configuration uses the default port of 8080.
6. Cluster name - Enter the Hadoop cluster name.
7. If you are using SSL, check the SSL Enabled checkbox.
8. User name - Enter an Ambari administrator user name.
9. Password - Enter the password for the Ambari administrator account.
10. Click Test Connection to verify the configuration.
11. Click Save to save the configuration.
12. **If you are using Hive 3+:** The Hadoop administrator must modify the configuration:
 - a. In the advanced configuration page in Ambari for Hive, remove any previous reference to the Guardium logger/appender from the log4j 2 configuration files (for example the beeline-log4j2, hive-exec-log4j2, hive-log4j2, and llap-cli-log4j2 files). Remove these lines:

```
# Configuration for Guardium integration with Ranger log4j logging.
log4j.appenders.guardlistener=org.apache.log4j.net.SocketAppender
log4j.appenders.guardlistener.Port=5555
log4j.appenders.guardlistener.RemoteHost=hw-cl4-01.guard.swg.usma.ibm.com
log4j.logger.xaaudit=ALL,guardlistener
```
 - b. Add these lines to the log4j 2 configuration files.

```
# audit logger
# Configuration for Guardium integration with Ranger log4j logging.
appender.guardlistener.type=Socket
appender.guardlistener.name=guardlistener
appender.guardlistener.port=5555
appender.guardlistener.host=9.32.164.237
appender.guardlistener.layout.type = SerializedLayout
logger.xaaudit.name=xaaudit
logger.xaaudit.level=INFO
logger.xaaudit.appenders.guardlistener.ref = guardlistener
```
 - c. Adjust the port and host for your environment. The host is the S-TAP you are using and the port is 5555 unless changed. If it is changed, it must match the log4j_port parameter value in the guard_tap.ini file.
 - d. Modify the log4j 2 configuration file with the same changes in four sections: beeline-log4j2, hive-exec-log4j2, hive-log4j2, and llap-cli-log4j2. The changes are:
 - add `guardlistener` to the list of appenders:
`appenders = console, DRFA, audittest, guardlistener`
 - add `xaaudit` to the list of loggers:
`NIOServerCnxn, ClientCnxnSocketNIO, DataNucleus, Datastore, JPOXgua, xaaudit`
 - e. Restart the HIVE service.
13. **If you are using version of Hive earlier than Hive 3+:** The Hadoop administrator must verify the configuration.

- a. # Configuration for Guardium integration with Ranger log4j logging.
`log4j.appenders.guardlistener=org.apache.log4j.net.SocketAppender
log4j.appenders.guardlistener.Port=5555
log4j.appenders.guardlistener.RemoteHost=<host name>
log4j.logger.xaaudit=ALL,guardlistener`
- b. Adjust the port and host for your environment. The host is the S-TAP you are using and the port is 5555 unless changed. If it is changed, it must match the log4j_port parameter value in the guard_tap.ini file.
- c. Verify the following settings in `custom`
`ranger-<service>-audit:`

```
xasecure.audit.destination.log4j=true  
xasecure.audit.destination.log4j.logger=xaudit
```

d. If any changes were made, restart the HIVE service.

14. If you are using Solr:

a. Register the Solr so that it can be monitored by using the script /usr/local/guardium/guard_stap/guard_log4j_listener_config.py. Enter this command, substituting your hostname:

```
./guard_log4j_listener_config.py -a <hostname> -b 8444 -u admin -p admin -c hw3cl1 -s solr -l 5555 -x enable --ssl
```

b. Install the ranger plugin and add the following lines to these files to enable log4j logging:

- /usr/cloudera-hdp-solr/xxx/cloudera-hdp-solr/solr/server/solr-webapp/webapp/WEB-INF/lib/ranger-solr-audit.xml
- /usr/cloudera-hdp-solr/xxx/cloudera-hdp-solr/solr/server/resources/ranger-solr-audit.xml

Lines to add to the files:

```
<!-- Log4j audit provider configuration -->  
    <property>  
        <name>xasecure.audit.destination.log4j</name>  
        <value>true</value>  
    </property>  
    <property>  
        <name>xasecure.audit.destination.log4j.logger</name>  
        <value>xaudit</value>  
    </property>  
    <property>  
        <name>xasecure.audit.log4j.is.enabled</name>  
        <value>true</value>  
    </property>
```

c. Restart the Solr.

Results

The new configuration is available from the Hadoop Monitoring page (marked with a green check mark icon). If the service does not display port information and the S-TAP status is **S-TAP not installed**, edit the configuration and specify a valid S-TAP.

Previous topic: [Linux-UNIX: Configure the Ranger plugins using Ambari](#)

Next topic: [Linux-UNIX: Install and configure S-TAPs](#)

Related information

- [Hortonworks Hadoop using Apache Ranger APIs](#)

Linux-UNIX: Install and configure S-TAPs

Install and configure S-TAPs for Ranger integration.

Before you begin

Review [Linux-UNIX: Planning the integration with Hortonworks and Apache Ranger](#) for information about S-TAP requirements and deployment options.

Procedure

1. Install S-TAPs and enable them for the Ranger integration.

You may need more than one S-TAP to handle the traffic, for example configure one S-TAP on the name node for HDFS, Hive and Kafka traffic and one S-TAP on the HBASE master node for all HBase traffic.

2. Configure guard_tap.ini for auditing.

a. Open guard_tap.ini in a text editor.

You must edit the file directly, as there is no UI or GIM support for these settings.

b. Add the parameters listed below.

Update the values to reflect your system.

```
; Settings for log4j  
logging.log4j_reader_enabled=1  
log4j_port=5555  
log4j_listen_address=0.0.0.0  
; Maximum number of connections to support from the log4j service  
log4j_num_connections=50
```

c. Restart the S-TAP after updating any settings.

What to do next

Install Guardium and Ranger policies. For monitoring and auditing, there is virtually no difference in policy rules when using Ranger than when using standard S-TAP monitoring for Hadoop. For more information, see [IBM Security Monitoring and Blocking for Hortonworks Hadoop Using Apache Ranger Integration](#).

Previous topic: [Linux-UNIX: Configure Guardium and Ranger communication](#)

Related reference

- [S-TAP configuration parameters for Hadoop](#)

Linux-UNIX: MongoDB IE configuration

View a typical insepction engine configuration, and flows for enabling and disabling A-TAP, and opening the SSL console for a MongoDB inspection engine.

Note: Redaction is not supported with or without SSL for Mongo 4.2 and higher.

MongoDB does not include OS_USER in the login packet, however you can use the UID chain to determine the DB_USER for reports. For more information, see [Linux-UNIX: UID chains](#).

Typical MongoDB inspection engine configuration

```
[DB_0]
connect_to_ip=127.0.0.1
db2_fix_pack_adjustment=20
db2_shmem_client_position=0
db2_shmem_size=131072
db2bp_path=NULL
db_exec_file=/usr/bin/mongod-guard-original
db_install_dir=/var/lib
db_type=MONGODB
db_user=mongod
encryption=0
db_version=9
instance_running=1
intercept_types=NULL
load_balanced=1
port_range_end=27017
port_range_start=27017
priority_count=20
real_db_port=27017
tap_identifier=MONGODB_mongo42-rhl7(27017,27017,DB_0)
tee_listen_port=0
unix_domain_socket_marker=NULL
networks=0.0.0.0/0.0.0.0
exclude_networks=
```

Activate and deactivate A-TAP for SSL traffic

Before activating A-TAP, you need to stop the MongoDB instance:

```
systemctl stop mongod
```

Activate A-TAP:

```
/usr/local/guardium/guard_stap/guardctl --db-user=mongod --db-type=mongodb --db-instance=mongo --db-base=/home/ibmuser --db-home=/usr activate
```

Restart the MongoDB instance:

```
systemctl start mongod
```

Set up mongo with TLS/SSL certificate and key

For example, on an instance with SSL and kerberization:

```
mongo --ssl --sslPEMKeyFile /etc/ssl/mongo40standalone-va.pem --sslPEMKeyPassword guardium --sslAllowInvalidCertificates --host <hostname> --port 27017 --authenticationMechanism=GSSAPI --authenticationDatabase='$external' --username <username>
```

Deactivating A-TAP

Before deactivating A-TAP, you need to stop the DB instance.

```
systemctl stop mongod
```

Deactivate A-TAP:

```
/usr/local/guardium/guard_stap/guardctl --db-user=mongod --db-type=mongodb --db-instance=mongo --db-base=/var/lib --db-home=/usr deactivate
```

Restart the MONGO DB instance:

```
systemctl start mongod
```

Linux-UNIX: Neo4J auditing configuration

Use a double proxy together with either K-TAP or PCAP to capture encrypted Neo4J traffic.

About this task

This procedure requires two proxies of either NGINX or HAProxy type. Both must both be located on the database.

The first proxy instance terminates the SSL and adds a proxy protocol to ports 7687 and 7473. The second proxy instance listens to the intermediate ports (17687 and 17473) and removes the proxy protocol. K-TAP or PCAP intercepts the traffic between the two proxy instances. Outgoing decrypted traffic from Proxy2 is sent to unencrypted Neo4j database ports (27687, 7474).

Procedure

1. Configure the database.

Neo4J advertises the ports it uses. The ports need to be changed to avoid conflicting with the proxy ports: Neo4J needs to have its port configuration changed and the proxy entry point ports need to be configured for advertising (requires version 3.5.0 or newer). In the neo4j configuration file: /home/neo4j/neo4j/conf/neo4j.conf, add/edit these lines. In this example the DB server is rh7u3x64t-ktap.databaseserver.

```
dbms.connector.bolt.listen_address=127.0.0.1:27687
dbms.connector.bolt.advertised_address=rh7u3x64t-ktap:7687
dbms.connector.http.listen_address=127.0.0.1:7474
dbms.connector.https.listen_address=127.0.0.1:27473
dbms.connector.https.advertised_address=rh7u3x64t-ktap:7473
```

2. Configure HAProxy. (Not required if you are using NGINX.)

In the HAProxy configuration file /etc/haproxy/haproxy.cfg:

- Enable the Proxy Protocol in Proxy1(HAProxy1) by adding the send-proxy keyword to the backend.
- Strip the Proxy protocol in Proxy2(HAProxy2) by adding accept-proxy to the frontend.

```
frontend main
    bind *:7687 ssl crt /home/neo4j/neo4j/certificates/neo4j.pem
    mode tcp
    default_backend send_proxy_protocol

backend send_proxy_protocol
    balance roundrobin
    server app1 127.0.0.1:17687 send-proxy

frontend strip_proxy_protocol
    bind 127.0.0.1:17687 accept-proxy
    mode tcp
    default_backend neo4j

backend neo4j
    balance roundrobin
    server app1 127.0.0.1:27687
```

3. Configure NGINX. (Not required if you are using HAProxy.)

For a TCP stream, the PROXY protocol can be enabled for connections between NGINX and an upstream server. To enable the PROXY protocol in Proxy1(Nginx1), include the proxy_protocol directive in a server block at the stream{} level in /etc/nginx/nginx.conf. NGINX terminates HTTPS traffic (the ssl_certificate and ssl_certificate_key directives) and proxies the decrypted data to a backend server. In Proxy2(Nginx2), add listen with proxy_protocol to receive the client's real IP forwarded with Proxy Protocol.

- Make sure that your NGINX installation includes the HTTP and Stream Real IP modules:

- nginx -V 2>&1 | grep -- 'http_realip_module'
- nginx -V 2>&1 | grep -- 'stream_realip_module'

- In the file /etc/nginx/nginx.conf, add:

```
stream {
    upstream neo4jweb {
        server localhost:7474;
    }
    upstream neo4jbolt {
        server localhost:27687;
    }

    server {
        listen 7473      ssl;
        proxy_pass      localhost:17473;
        proxy_protocol  on;
        ssl_certificate /home/neo4j/neo4j/certificates/neo4j.cert;
        ssl_certificate_key /home/neo4j/neo4j/certificates/neo4j.key;
    }
    server {
        listen 7687      ssl;
        proxy_pass      localhost:17687;
        proxy_protocol  on;
        ssl_certificate /home/neo4j/neo4j/certificates/neo4j.cert;
        ssl_certificate_key /home/neo4j/neo4j/certificates/neo4j.key;
    }
    server {
        listen 17473     proxy_protocol;
        proxy_pass      neo4jweb;
    }
    server {
        listen 17687     proxy_protocol;
        proxy_pass      neo4jbolt;
    }
}
```

4. Configure the network.

Verify that all traffic from the client is sent to Proxy1. Any traffic that does not go from Proxy2 to DB is dropped. This requires IPTABLE setup. Use this script neo4j_firewall.sh to set up the IPTABLES:

```

#!/bin/sh

# Remove any existing jumps to our custom chains
iptables -D INPUT -j chain-neo4j-incoming
iptables -D OUTPUT -j chain-neo4j-outgoing

# Clean any existing custom chains
iptables -F chain-neo4j-incoming
iptables -F chain-neo4j-outgoing
iptables -X chain-neo4j-incoming
iptables -X chain-neo4j-outgoing
iptables -N chain-neo4j-incoming
iptables -N chain-neo4j-outgoing

# Define external(proxy1), proxy2, ssl and no ssl ports
no_ssl_port_prefix=2
proxy2_port_prefix=1
port_list=0

# Pass in all arguments, please see bottom usage.
for i in "$@" ; do
    # set the port prefix
    if echo $i | grep '^-' > /dev/null; then
        if echo $i | grep '^--port_list$' > /dev/null; then
            port_list=999
        fi
    elif [ "X${port_list}" = "X999" ]; then
        external_port=${i}
        proxy2_port=${proxy2_port_prefix}${i}
        no_ssl_port=${no_ssl_port_prefix}${i}
        if [ "${external_port}" = "7473" ]; then
            no_ssl_port=7474
        fi
    ######
    # INCOMING RULES

    # Allow loopback access to intermediate ports so that proxy1 can
    # route traffic to proxy2
    iptables -A chain-neo4j-incoming -i lo -p tcp --dport ${proxy2_port} -j ACCEPT

    # Disallow external access to proxy2
    iptables -A chain-neo4j-incoming -p tcp --dport ${proxy2_port} -j REJECT

    # Allow loopback access to unencrypted ports so that proxy2 can
    # route traffic to DB
    iptables -A chain-neo4j-incoming -i lo -p tcp --dport ${no_ssl_port} -j ACCEPT

    # Disallow direct access to unencrypted ports
    iptables -A chain-neo4j-incoming -p tcp --dport ${no_ssl_port} -j REJECT

    # Allow access to proxy1
    iptables -A chain-neo4j-incoming -p tcp --dport ${external_port} -j ACCEPT
    ######
    # OUTGOING RULES

    # Allow loopback access to unencrypted ports to allow routing from proxy2 to
    # DB (proxy2 runs under neo4j UID)
    iptables -A chain-neo4j-outgoing -o lo -p tcp --dport ${no_ssl_port} -m owner --uid neo4j -j ACCEPT

    # Allow loopback access to intermediate ports to allow routing from proxy1 to
    # proxy2 (proxy1 runs under neo4j UID)
    iptables -A chain-neo4j-outgoing -o lo -p tcp --dport ${proxy2_port} -m owner --uid neo4j -j ACCEPT

    # Disallow loopback access to unencrypted ports to prevent local clients from
    # skipping interception
    iptables -A chain-neo4j-outgoing -o lo -p tcp --dport ${no_ssl_port} -j REJECT
fi
done

if [ "${port_list}" = "0" ]; then
    echo "usage: /root/set_firewall.sh -port_list [external port list]"
    echo "for example /root/set_firewall.sh -port_list 7473 7687"
fi

# Firewall chains need to return at the end
iptables -A chain-neo4j-incoming -j RETURN
iptables -A chain-neo4j-outgoing -j RETURN

# Hook the main rules up to the chains
iptables -A INPUT -j chain-neo4j-incoming
iptables -A OUTPUT -j chain-neo4j-outgoing

```

5. Configure the S-TAP.

When configuring the proxy instances, the first instance terminates the encryption and adds the proxy-protocol for Guardium to collect the traffic and be able to attribute the correct analyzed client IP. The second instance removes the proxy-protocol, to not break the connection to the database. Configure the inspection engine to collect the traffic between the two proxy instances. For example, if you are using the example configurations above, then the ports to collect for Neo4j are 17473, 17687.

- If you are using K-TAP, modify the guard_tap.ini file:
 - IE parameters

```
[DB_0]
db_type=NEO4J
```

```

port_range_end=17473
port_range_start=17473
real_db_port=17473
networks=127.0.0.1/255.255.255.255,9.70.165.199/255.255.255.255

[DB_1]
db_type=NEO4J
port_range_end=17687
port_range_start=17687
real_db_port=17687
networks=127.0.0.1/255.255.255.255,9.70.165.199/255.255.255.255

• If you are using PCAP, modify the guard_tap.ini file:
  • TAP properties

  devices=ens32,lo
  ktap_installed=0

  • IE parameters

  [DB_0]
  db_type=NEO4J
  port_range_end=17473
  port_range_start=17473
  real_db_port=17473

  [DB_1]
  db_type=NEO4J
  port_range_end=17687
  port_range_start=17687
  real_db_port=17687

```

Linux-UNIX: Oracle Connection Manager configuration to monitor encrypted traffic

You can use the Oracle Connection Manager to monitor encrypted traffic, without A-TAP.

Before you begin

- S-TAP 10.x or higher is installed in the Oracle database server.
- Oracle Connection Manager v18.3 is installed and configured for SSL.

About this task

The Oracle Connection Manager is a proxy server that forwards connection requests to databases or other proxy servers. It operates on the session level. It usually resides on a computer separate from the database server and client computers. It is a custom installation option on the Clientdisk. The primary functions of Oracle Connection Manager are:

- Access control: to use rule-based configuration to filter user-specified client requests and accept others.
- Session multiplexing: to funnel multiple client sessions through a network connection to a shared server destination.
- Hardening security: can be setup as proxy server between public and trusted network.

The public (open external) network includes the web client, firewalls, and application server. The trusted (private internal) network is non-routable and exists only between the connection manager and database server. It is recommended for OCM that most actual database services, like the database listener and administrative applications like Oracle Grid Control, should be configured to run on the private network where they cannot be subjected to random port scans.

Configure the OCM in one of these models:

- [Linux-UNIX: Install and configure the Oracle Connection Manager on the database server](#)
recommended. Cant be directly to data base but all clients connected to OCM.
- [Linux-UNIX: Install and configure the Oracle Connection Manager in an Oracle RAC environment](#)
Oracle RAC cluster environments are usually set up within a private (trusted) network. Data should be only encrypted for remote clients' connections.
- [Linux-UNIX: Install and configure the Oracle Connection Manager on a remote server](#)
There are transfers of unencrypted data between the OCM and the actual database server. Install and configure the Oracle Connection Manager (OCM) on a separate server between the public network and the trusted (private) network when required for security reasons.

Linux-UNIX: Install and configure the Oracle Connection Manager on the database server

recommended. Cant be directly to data base but all clients connected to OCM.

Procedure

1. Configure the Oracle Connection Manager (OCM) environment.
 - Configure the Listener for OCM for TCPS and TCP protocols with the remote server hostname or the IP address in the file cman.ora.
 - Configure the file cman.ora with the standard parameter list for OCM and enable_ip_forwarding=yes. The rule list should include the source configured for the Oracle Database hostname or IP and destination to local host.
 - Configure sqlnet.ora in the OCM environment for SSL connections.

Example of cman.ora file:

```

cman=
(configuration=
(address=(protocol=tcps) (host=<DB_server_hostname/IP>) (port=1552))
(address=(protocol=tcp) (host=<DB_server_hostname/IP>) (port=1551))
(parameter_list =
(aso_authentication_filter=off)
(connection_statistics=yes)
(log_level=off)
(enable_ip_forwarding=yes)
(max_connections=256)
(idle_timeout=0)
(inbound_connect_timeout=0)
(
session_timeout=0)
(outbound_connect_timeout=0)
(max_gateway_processes=16)
(min_gateway_processes=2)
(remote_admin=on)
(trace_level=off)
(trace_timestamp=off)
(trace_filelen=1000)
(tr
ce_fileno=1)
(max_cmctl_sessions=4)
(event_group=init_and_term,memory_ops)
)
(rule_list=
(rule=(src=<DB_server_hostname/IP>) (dst=127.0.0.1) (srv=cmon) (act=accept))
(rule=(src=127.0.0.1) (dst=*) (srv=*) (act=reject))
(rule=(src=<DB_server_hostname/IP>) (dst=*) (srv=*) (act=reject)
(rule=(src=*) (dst=*) (srv=*) (act=accept))
)
)

WALLET_LOCATION =
(SOURCE =
(METHOD = FILE)
(METHOD_DATA =
(DIRECTORY = /home/cman/app/cman/produ
ct/18.0.0/client_1/network/admin/wallet)
)
)

```

2. Configure the Oracle server.

- Local Listeners for the database server should be listen only TCP ports for the localhost address.
- Remote listener should be set with parameters from the file cman.ora in the tnsnames.ora file.

Example of tnsnames.ora file:

```

LISTENER_CMAN =
(DESCRIPTION_LIST =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP) (HOST = <DB_server_hostname/IP>) (PORT = 1551))
(ADDRESS = (PROTOCOL = TCPS) (HOST = <
DB_server_hostname/IP>) (PORT = 1552))
)
)
LISTENER =
(DESCRIPTION_LIST =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP) (HOST = 127.0.0.1) (PORT = 1528))
)
)

```

LISTENER_CMAN is an alias for your Remote Listener and LISTENER is an alias for your Local Listener in this case.

3. Configure the Oracle clients.

- The connection string in Oracle client environments should be set for TCPS protocol with a designated port, set for that protocol in the OCM environment and hostname or IP specified for Remote Listener with the associated SERVICE_NAME.

This configuration prevents local connections from connecting via CMAN since local traffic should not be encrypted and the S-TAP should be able to capture the UID chain.

Linux-UNIX: Install and configure the Oracle Connection Manager in an Oracle RAC environment

Oracle RAC cluster environments are usually set up within a private (trusted) network. Data should be only encrypted for remote clients' connections.

Procedure

Configure the Oracle Connection Manager (OCM) environment on the main Oracle RAC node or on each node for high availability.

- Configure the Listener for OCM for TCPS and TCP protocols with the remote server hostname or Ithe P address in the file cman.ora.
- Configure the cman.ora file with standard parameter list for OCM and enable_ip_forwarding=yes. The rule list should include a source configured for server hostname or IP and destination to SCAN - LISTENER hostname or IP.
- In the cman.ora file, set the parameter REGISTRATION_INVITED_NODES with node(s) hostname(s) or IP(s). This parameter also accepts wildcards as values for group of IPs.
- Configure the file sqlnet.ora in the OCM environment for SSL connections

- Configure client's connections to connect to RAC instances using OCM and SCAN_LISTENER hostnames and corresponding ports.

Example of cman.ora file:

```
cman=
(configuration=(address=(protocol=tcps) (host=<CMAN_HOST/IP>) (port=1552))
(address=(protocol=tcp) (host=<CMAN_HOST/IP>) (port=1551))
(parameter_list =
(aso_authentication_filter=off)
(connection_statistics=yes)
(log_level=off)
(enable_ip_forwarding=yes)
(max_connections=256)
(idle_timeout=0)
(inbound_connect_timeout=0)
(session_timeout=0)
(outbound_connect_timeout=0)
(max_gateway_processes=16)
(min_gateway_processes=2)
(remote_admin=on)
(trace_level=off)
(trace_timestamp=off)
(trace_filelen=1000)
(trace_filenr=1)
(max_cmt_sessions=4)
(event_group=init_and_term,memory_ops)
(REGISTRATION_INVITED_NODES =node1_host,node2_host,node3_host/ IPs)
)

(rule_list=(rule=(src=CMAN_HOST) (dst=*) (srv=cmon) (act=accept))
(rule=(src=CMAN_HOST) (dst=*) (srv=*) (act=reject))
(rule=(src=127.0.0.1) (dst=*) (srv=cmon) (act=accept))
(rule=(src=127.0.0.1) (dst=*) (srv=*) (act=reject))
(rule=(src=:1) (dst=*) (srv=cmon) (act=accept))
(rule=(src=:1) (dst=*) (srv=*) (act=reject))
(rule=(src=*) (dst=SCAN_LISTENER_HOST/IP) (srv=DB_SERVICE_NAME) (act=accept))
)

)

WALLET_LOCATION =
(SOURCE =
(METHOD = FILE)
(METHOD_DATA =
(DIRECTORY = /home/cman/app/cman/product/18.0.0/client_1/network/admin/wallet)
)
)
```

Example of tnsnames.ora file:

```
Connection_String=
(description=
(source_route=yes)
(address_list=
(address=(protocol=tcps) (host=CMAN_HOST) (port=1552))
(address=(protocol=tcp) (host=SCAN_LISTENER_HOST) (port=SCAN_PORT) )
)
(connect_data=(service_name=DB_SERVICE_NAME))
(SECURITY=(SSL_SERVER_CERT_DN="cn=Unit,cn=Organisation,dc=us,dc=com")
)
```

Linux-UNIX: Install and configure the Oracle Connection Manager on a remote server

There are transfers of unencrypted data between the OCM and the actual database server. Install and configure the Oracle Connection Manager (OCM) on a separate server between the public network and the trusted (private) network when required for security reasons.

Procedure

1. Configure the Oracle Connection Manager (OCM) environment:

- Configure the Listener for OCM for TCPS and TCP protocols with the remote server hostname or the IP address in the file cman.ora.
- Configure the file cman.ora with the standard parameter list for OCM and enable_ip_forwarding=yes. The rule list should include the source configured for the remote server Hostname or IP and the destination to the Oracle Database hostname or IP.
- In the file cman.ora set the parameter REGISTRATION_INVITED_NODES with the Database(s) hostname(s) or IP(s). This parameter also accepts a wildcard as a value for group of IPs.
- Configure sqtnet.ora in the OCM environment for SSL connections.

Example of cman.ora file:

```
cman=
(configuration=
(address=(protocol=tcps) (host=<Remote_hostname/IP>) (port=1552))
(address=(protocol=tcp) (host=<Remote_hostname/IP>) (port=1551))
(parameter_list=(aso_authentication_filter=off)
(connection_statistics=yes)
(log_level=off)
(enable_ip_forwarding=yes)
(max_connections=256)
(idle_timeout=0)
```

```

(inbound_connect_timeout=0)
(session_timeout=0)
(outbound_connect_timeout=0)
(max_gateway_processes=16)
(min_gateway_processes=2)
(remote_admin=on)
(trace_level=off)
(trace_timestamp=off)
(trace_filelen=1000)
(trace_fileno=1)
(max_cmctl_sessions=4)
(event_group=init_and_term,memory_ops)
(REGISTRATION_INVITED_NODES = DB_server_hostname/IP)
)
(rule_list=(rule=(src=<Remote_hostname/IP>) (dst=*) (srv=cmon) (act=accept))
(rule=(src=<DB_server_hostname/IP>) (dst=*) (srv=*) (act=reject))
(rule=(src=*) (dst=*) (srv=*) (act=accept)))
)
WALLET_LOCATION =
(SOURCE =
(METHOD = FILE)
(METHOD_DATA =
(DIRECTORY = /home/cman/app/cman/product/18.0.0/client_1/network/admin/wallet))

```

2. Configure the Oracle server.

- Local Listeners for the database server should be only listen TCP ports with DB_server_hostname/IPAddress
- Remote listener should be set with parameters from cman.ora file in the tnsnames.ora file

Example of tnsnames.ora file:

```

LISTENER_CMAN =
(DESCRIBE
PTION_LIST =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP) (HOST = <Remote_hostname/IP>) (PORT = 1551))
(ADDRESS = (PROTOCOL = TCPS) (HOST = <Remote_hostname/IP>) (PORT = 1552))
)
)
LISTENER =
(DESCRIPTION_LIST =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP) (HOST = DB_server_hostname/IP) (PORT = 1528))
)
)

```

LISTENER_CMAN is alias for your Remote Listener, and LISTENER is alias for your Local Listener in this case.

3. Configure Oracle clients.

- The connection string in Oracle client environments should be set for TCPS protocol with designated port set for that protocol in OCM environment and hostname or IP specified for Remote Listener with associated SERVICE_NAME.

Ports in the Inspection Engine for Oracle should match the values set for Local Listener only.

Linux-UNIX: Oracle IE configuration

View a typical configuration for an inspection engine on an Oracle database.

If the database is up during the S-TAP installation, it should automatically set up the inspection engines for Oracle. In some complicated cases the auto-discovery process may not configure the inspection engine for a Unix S-TAP, and manual configuration is required.

Inspection engine parameters:

```

connect_to_ip=127.0.0.1,::1
db_exec_file=<FULL_PATH_TO_ORACLE_BINARY>
db_install_dir=<ORACLE_OS_USER_HOME>
db_type=oracle
db_user=<ORACLE_OS_USER>
encryption=0
db_version=<DB_VERSION>
instance_running=1
intercept_types=NULL
load_balanced=1
port_range_end=<VALUE_FOR_PORT_RANGE(END)>
port_range_start=<VALUE_FOR_PORT_RANGE(START)>
priority_count=20
real_db_port=<VALUE_FOR_PORT>
tap_identifier=<COULD_BE_CUSTOM_OR_EMPTY_DURING_SETUP>
tee_listen_port=0
unix_domain_socket_marker=NULL
networks=0.0.0.0/0.0.0.0,::/0
exclude_networks=

```

Example:

```

DB_0:
connect_to_ip=127.0.0.1,::1
db2_fix_pack_adjustment=20
db2_shmem_client_position=0
db2_shmem_size=131072
db2bp_path=NULL
db_exec_file=/${ORACLE_HOME}/bin/oracle
db_install_dir=/home/oracle18

```

```

db_type=oracle
db_user=oracle18
encryption=0
db_version=18
instance_running=1
intercept_types=NULL
load_balanced=1
port_range_end=1525
port_range_start=1520
priority_count=20
real_db_port=1521
tap_identifier=oracle_9.70.147.74(1521,1521,DB_0)
tee_listen_port=0
unix_domain_socket_marker=ORCL
networks=0.0.0.0/0.0.0.0,::/0
exclude_networks=

```

Linux-UNIX: Configuring S-TAP interception using Oracle Unified Audit

Use Oracle Unified Auditing (OUA) to capture user activities in Oracle database environments based on Oracle Unified Audit policies. All captured activities are stored in specific tables. Linux S-TAP x86_64 can dynamically load and use Oracle-provided libraries to connect to the configured Oracle services. The S-TAP can then pull data from the unified auditing tables, and send data to Guardium collectors.

Before you begin

With Oracle Unified Auditing, the S-TAP does not need to be on the same server where Oracle Unified Auditing is set up. It can be installed on any Linux x86_64-based server, either the same server (if Oracle is running on a Linux x86_64 platform) or a remote server. If the S-TAP is installed on a remote server, it captures database activities remotely.

If Oracle Instant Client is not already installed and configured, the root user must take the following steps :

1. Download Oracle Instant Client rpm from the Oracle website at <https://www.oracle.com/database/technologies/instant-client/linux-x86-64-downloads.html>.
2. Install the Oracle Instant Client Basic rpm on the Linux server where you install the S-TAP. For example:

```
rpm -ivh oracle-instantclient-basic-21.10.0.0.0-1.el8.x86_64.rpm
```

3. The installation process installs the Oracle libraries and creates the TNS_ADMIN path for Oracle Instant client. Add tnsnames.ora or ldap.ora files that contain content for Oracle Database connections that the S-TAP will monitor under the TNS_ADMIN path. The TNS_ADMIN path might be similar to the following example:

```
/usr/lib/oracle/21/client64/lib/network/admin
```

Note: The Oracle Instant Client must be installed on the same system where you install the S-TAP.

About this task

Oracle Unified Auditing with an S-TAP has the following requirements:

- Using Guardium® S-TAP with the Oracle Unified Auditing method requires Oracle database 18c and higher.
- Oracle Instant Client must be version 18 or higher.
- Unified auditing must be enabled in any Oracle database instances that you want to monitor by this method.
- The designated user for S-TAP must either be created for Oracle database access or you can use an existing user with sysdba privileges.

Procedure

1. Create a designated database user (with minimal privileges) for S-TAP as follows,
 - a. Connect to Oracle by using the `sysdba` account. For this example, the Oracle Unified Audit user is called `guardium` (`password = password`).

```

CREATE USER guardium IDENTIFIED BY password
GRANT CONNECT, RESOURCE to guardium;
GRANT SELECT ANY DICTIONARY TO guardium;
exec DBMS_NETWORK_ACL_ADMIN.APPEND_HOST_ACE(host => 'localhost', ace  => xs$ace_type(privilege_list =>
xs$name_list('connect', 'resolve'), principal_name  => 'guardium', principal_type => xs_acl.ptype_db));

```

- b. You can verify your new user's privileges by connecting to the Oracle instance with the specified name and credentials. Run following statements:

```

select count(*) from AUDSYS.AUD$UNIFIED;
SELECT UTL_INADDR.get_host_address FROM DUAL;

```

If no errors are returned, then the user has appropriate privileges for Oracle Unified Auditing S-TAP interception.

Note: Instead of creating a new user, you can use an existing user that has `sysdba` privileges.

2. From either the Guardium GUI or the `guard_tap.ini` file, set the following parameters.

- From the Guardium GUI, browse to `Manage > Activity Monitoring > S-TAP Control`. In the Details section of S-TAP Control, make the following updates,
 - LD library paths - The path to the Oracle Instant Client libraries that are installed on the system. For example,

```
/usr/lib/oracle/19.8/client64/lib
```

- SQL configuration properties directory - The TNS_ADMIN path for Oracle Instant client. For example,

```
/usr/lib/oracle/19.8/client64/lib/network/admin
```

- From `guard_tap.ini`, set the following parameters,

```
ld_library_paths=/usr/lib/oracle/19.8/client64/lib
sqlc_properties_dir=/usr/lib/oracle/19.8/client64/lib/network/admin
```

3. Add the SQL configuration. This configuration is similar to inspection engines. Use one of the following methods:

- From the S-TAP Control page, take the following steps:
 - Click .
 - Click Add SQL Configuration.
 - Complete the details and then click Add.
 - Finally, click Apply to apply your changes.
- From the CLI, call the `create_sql_configuration` GrdAPI. For more information about parameters, see [create_sql_configuration](#).
- From `guard_tap.ini`, add one section for each database instance at the end of the file:

```
[SQLC_<0,1,2...>]
data_pull_interval=300
data_pull_num_rows=100
db_type=oracle
instance=on8pgrel
timeout=300000
username=username
```

4. Store the username and password pair for the designated user that you created (or for an existing user).

You can store the username and password pair from either the Guardium GuardAPI or from the Guardium S-TAP Control page in the GUI.

- To use the CLI, run the `store_sql_credentials` GuardAPI command from the CLI. For example,

```
grdapic store_sql_credentials staphost=STAPHOST username=guardium password=password
```
- From the S-TAP Control page in the Guardium GUI,
 - Click the Send Command , then select Store SQL credentials from the drop-down list.
 - Enter the username and password, and then click Apply.

Note: You can also update the password by entering an existing username and a new password.

Related reference

- [create_sql_configuration](#)
- [delete_sql_configuration](#)
- [store_sql_credentials](#)
- [Linux-UNIX: Oracle Unified Auditing parameters](#)

Related information

- [Oracle Unified Audit Activity](#)
- [Oracle Unified Audit \(S-TAP Configuration\) Activity](#)

Linux-UNIX: Redis configuration

Redis TCP protocol is supported by an S-TAP installed on a Redis server. If Redis is set up with SSL/TLS encryption, you need two proxies using HAProxy Load Balancer.

Capturing SSL Redis protocol activities

Capturing SSL Redis protocol activities requires two proxies using HAProxy Load Balancer. They must be set up and configured on the same database server. S-TAP can be set up with K-TAP or PCAP. K-TAP or PCAP intercepts the traffic between the two proxy ports.

Guidelines: Double-proxy set up with:

- HAProxy Load Balancer input port 18345
- Middle port 18346 where activities are captured
- Port 18347 output port, which is configured also for the Redis connection

The Redis certificate can be used, for convenience. An example for Redis connection after HAProxy Load Balancer setup:

```
redis-cli -h `hostname` -p 18345 --tls --cacert /etc/opt/redislabs/proxy_cert.pem
```

Configure the HAProxy Load Balancer in a configuration file that is typically located at `/etc/haproxy/haproxy.cfg`. For example:

```
#####
main frontend which proxys to the backends
#####
frontend main_in
bind 0.0.0.0:18345 ssl crt /etc/haproxy.pem
mode tcp
use_backend intermediate_out
backend intermediate_out
server output 127.0.0.1:18346 send-proxy
frontend intermediate_in
bind 0.0.0.0:18346 accept-proxy
mode tcp
use_backend main_out
backend main_out
server output 127.0.0.1:18347 ssl verify none crt /etc/haproxy.pem
```

Typical inspection engine configuration

```
[DB_0]
connect_to_ip=127.0.0.1,::1
db2_fix_pack_adjustment=80
db2_shmem_client_position=0
db2_shmem_size=131072
db2bp_path=NULL
db_exec_file=/opt/redislabs/bin/redis-server
db_install_dir=/opt/redislabs/
db_type=REDIS
db_user=redislabs
encryption=0
db_version=0
instance_running=1
intercept_types=NULL
load_balanced=1
port_range_end=18346
port_range_start=18340
priority_count=20
real_db_port=18346
tap_identifier=REDIS_STAP
tee_listen_port=0
unix_domain_socket_marker=NULL
networks=0.0.0.0/0.0.0.0,::/0
exclude_networks=
```

Linux-UNIX: S-TAP operation and performance

- [Linux-UNIX: Stopping S-TAP using GIM](#)
With GIM, you can stop the S-TAP without logging into the database server.
- [Linux-UNIX: Starting S-TAP using GIM](#)
With GIM, you can start the S-TAP without logging into the database server.
- [Linux-UNIX: Start and stop S-TAP and GIM processes for various OS types/versions](#)
Depending on the operating system type and version there are different methods used to start and stop Guardium processes. Learn how to start and stop the S-TAP and GIM processes.
- [Linux-UNIX: Using guard-config-update to start, restart, and stop S-TAP, and view status](#)
You can use the guard-config-update utility to update your S-TAP configuration (without using the GUI), whether S-TAP was installed with GIM, RPM, or shell.
- [Linux-UNIX: Optimizing your configuration for high load](#)
Guardium has two options for managing a high load between the data sources and the collectors, which can be implemented individually, or together.
- [Linux-UNIX: Alerts on uninstalled S-TAPs](#)
Uninstalling an S-TAP might be evidence of harmful activity. The predefined S-TAP Uninstall Alert notifies when an S-TAP is uninstalled. You can view the S-TAP Uninstall Events report in My Dashboards.
- [Linux-UNIX: Deleting inactive S-TAPs in a centralized environment](#)
You can use a cron job on the central manager to delete all inactive S-TAP instances.
- [Linux-UNIX: Monitoring S-TAP in the GUI](#)
Use these standard reports and views to monitor your S-TAP status in the GUI.
- [Linux-UNIX: S-TAP logs](#)
The UNIX S-TAP has a few log files.
- [Linux-UNIX: Viewing S-TAP debug details on the database](#)
You can view some S-TAP debug details on the database itself, by using the .stap_state file, located in the S-TAP installation directory.
- [Linux-UNIX: Determine the S-TAP version](#)
- [Linux-UNIX: S-TAP statistics](#)
S-TAP statistics are easily viewed in the predefined S-TAP and External S-TAP Statistics report.
- [Linux-UNIX: S-TAP Monitor \(guard_monitor\)](#)
The S-TAP Watchdog (guard_monitor) monitors S-TAP performance and responsiveness. You can configure specific actions that are triggered when the S-TAP exceeds certain thresholds.
- [Linux-UNIX: Troubleshooting S-TAP problems](#)
You can use the S-TAP Status monitor tab of the System View to begin investigating any problems. Sometimes you might need to use other tools, particularly if you are monitoring databases for which the inspection engines cannot be verified.

Linux-UNIX: Stopping S-TAP using GIM

With GIM, you can stop the S-TAP without logging into the database server.

About this task

Use the following steps to change the STAP_ENABLED parameter and stop the S-TAP on the database server.

Procedure

1. Navigate to **Manage > Module Installation > Set up by Client**.
2. In the Choose bundle section, select your S-TAP bundle. Click Next.
After selecting a software bundle, the Selected bundle action column indicates the action that will be performed for each client. You can stop the S-TAPs that have the status Update parameters.
3. In the Choose parameters section, type **STAP_ENABLED** and type in the value 0. Click Next.

4. Click OK to stop the S-TAP now, or use the  icon to schedule the stop time, then click OK.

Linux-UNIX: Starting S-TAP using GIM

With GIM, you can start the S-TAP without logging into the database server.

About this task

Use the following steps to change the STAP_ENABLED parameter and start the S-TAP on the database server.

Procedure

1. Navigate to Manage > Module Installation > Set up by Client.
2. In the Choose clients section, select the database servers whose S-TAPs you want to start. Select individual clients using check boxes in the table, or use the Select client group menu to select a group of clients. Click Next to continue.
3. In the Choose parameters section, type STAP_ENABLED and type in the value 1. Click Next.
4. Click OK to start the S-TAP now, or use the  icon to schedule the start time, then click OK.

Linux-UNIX: Start and stop S-TAP and GIM processes for various OS types/versions

Depending on the operating system type and version there are different methods used to start and stop Guardium processes. Learn how to start and stop the S-TAP and GIM processes.

First identify the method relevant for your database in [Table 1](#), then proceed to the relevant sub-section for the relevant commands.

When you stop the S-TAP or GIM from the database command line, the operating starts it again automatically.

Tip: You can also use the `guard-config-update` utility to start and stop the S-TAP, whether it was installed with GIM, RPM, or shell. When you use `guard-config-update`, you don't need to know the relevant commands. See [Linux-UNIX: Using guard-config-update to start, restart, and stop S-TAP, and view status](#).

Table 1. Startup facility based on OS and version

| OS | Version | Initialization method |
|---------|---------|-----------------------|
| AIX | all | inittab |
| Debian | all | systemd |
| HP-UX | all | inittab |
| RHEL | 5 | inittab |
| RHEL | 6 | upstart |
| RHEL | 7 | systemd |
| RHEL | 8 | systemd |
| SUSE | 11 | inittab |
| SUSE | 12 | systemd |
| SUSE | 15 | systemd |
| Ubuntu | 14.04 | upstart |
| Ubuntu | 16.04 | systemd |
| Ubuntu | 18.04 | systemd |
| Solaris | 5.10 | service |

- [Linux-UNIX: Start and stop methods for inittab](#)
To start or stop processes in inittab, you need to edit the file /etc/inittab.
- [Linux-UNIX: Start and stop methods for Solaris services](#)
Learn how to start and stop S-TAP and GIM processes for Solaris services.
- [Linux-UNIX: Start and stop methods for systemd](#)
Learn how to start and stop S-TAP and GIM processes with systemd services.
- [Linux-UNIX: Start and stop methods for upstart](#)
Learn how to start and stop S-TAP and GIM processes with upstart services.

Linux-UNIX: Start and stop methods for inittab

To start or stop processes in inittab, you need to edit the file /etc/inittab.

1. Add or erase a hash sign # to comment or comment out the service. In AIX, use a colon (:) instead.
2. Run init q to make the changes effective.

Changes to the file depend on the installation path and the version. Typical examples are:

```
gim:2345:respawn:/usr/bin/perl /usr/local/IBM/modules/GIM/11.2.0.0_r108796_1-1590008051/gim_client.pl
```

```
gsvr:2345:respawn:/usr/local/IBM/modules/perl /usr/local/IBM/modules/SUPERVISOR/11.2.0.0_r108796_1-1590008053/guard_supervisor
```

Linux-UNIX: Start and stop methods for Solaris services

Learn how to start and stop S-TAP and GIM processes for Solaris services.

Table 1. svc commands to start and stop processes

| Action | S-TAP commands |
|-------------------------------|---|
| Start S-TAP | <code>svcadm -v enable guard_utap</code> |
| Stop S-TAP | <code>svcadm -v disable guard_utap</code> |
| Verify S-TAP status | <code>svcs grep guard_utap</code> |
| Start GIM, supervisor | <code>svcadm -v enable guard_gim</code>
<code>svcadm -v enable guard_gsvr</code> |
| Stop GIM, supervisor | <code>svcadm -v disable guard_gim</code>
<code>svcadm -v disable guard_gsvr</code> |
| Verify GIM, supervisor status | <code>svcs grep guard</code> |

Linux-UNIX: Start and stop methods for systemd

Learn how to start and stop S-TAP and GIM processes with systemd services.

Table 1. systemd commands to start and stop processes

| Action | S-TAP commands |
|-------------------------------|---|
| Start S-TAP | <code>systemctl start guard_utap.service</code> |
| Stop S-TAP | <code>systemctl stop guard_utap.service</code> |
| Verify S-TAP status | <code>systemctl -t service -a grep guard_utap</code> |
| Start GIM, supervisor | <code>systemctl start guard_gim.service</code>
<code>systemctl start guard_gsvr.service</code> |
| Stop GIM, supervisor | <code>systemctl stop guard_gim.service</code>
<code>systemctl stop guard_gsvr.service</code> |
| Verify GIM, supervisor status | <code>systemctl -t service -a grep guard</code> |

Linux-UNIX: Start and stop methods for upstart

Learn how to start and stop S-TAP and GIM processes with upstart services.

- Run `initctl list` to list the upstart services.
- Run `start <service_name>` to start the service.
- Run `"stop <service_name>"` to stop the service.

Table 1. upstart commands to start and stop processes

| Action | S-TAP commands |
|--|---|
| Start S-TAP | <code>start utap</code> |
| Stop S-TAP | <code>stop utap</code> |
| Verify S-TAP status | <code>status utap</code> |
| Identify the service name of GIM and supervisor: | <code>initctl list grep gim</code>
<code>initctl list grep gsvr</code> |
| Start GIM, supervisor | <code>start gim_<revision#></code>
<code>start gsvr_<revision#></code>
For example: <code>start gim_56789</code> |
| Stop GIM, supervisor | <code>stop gim_<revision#></code>
<code>stop gsvr_<revision#></code>
For example: <code>stop gim_56789</code> |
| Verify GIM, supervisor status | <code>status gim_<revision#></code>
<code>status gsvr_<revision#></code>
For example: <code>status gim_56789</code> |

Linux-UNIX: Using guard-config-update to start, restart, and stop S-TAP, and view status

You can use the `guard-config-update` utility to update your S-TAP configuration (without using the GUI), whether S-TAP was installed with GIM, RPM, or shell.

Before you begin

For all commands, <filepath> is the path to the guard-config-update utility, where the path depends on your installation type, as follows,

- Shell installation - Default path = /usr/local/guardium/bin/guard-config-update
- GIM installation - Default path = /usr/local/modules/STAP/current/guard-config-update
- RPM installation - Default path = /opt/guardium/bin/guard-config-update

Note: If your site does not use the default filepath, make sure you know the correct location for the guard-config-update utility.

Procedure

1. Log in to the database server as root.
2. To stop S-TAP:

```
# <filepath>/guard-config-update --stop stap
Stopping STAP
utap stop/waiting
#
```

3. To start S-TAP:

```
# <filepath>/guard-config-update --start stap
Starting STAP
utap start/running, process 14969
#
```

4. To restart S-TAP:

```
# <filepath>/guard-config-update --restart stap
Restarting STAP
utap start/running, process 15331
#
```

5. To show S-TAP status:

```
# <filepath>/guard-config-update --status
Running services:
  STAP : root      15331      1 0 14:14 ?          00:00:00 /usr/local/guardium/guard_stap/guard_stap
  /usr/local/guardium/guard_stap/guard_tap.ini

Services configured:
  STAP : enabled
  TEE  : disabled
  MONITOR: disabled

DAM plaintext connections:
  tcp      0      0 9.70.147.17:24007      9.32.132.217:16016      ESTABLISHED
  tcp      0      0 9.70.147.17:51791      9.32.132.217:16016      TIME_WAIT

DAM TLS connections:
None
FAM plaintext connections:
None
FAM TLS connections:
None

TLS is disabled

STAP debug is not enabled via config

System info:
  RESTART METHOD: upstart
#
#
```

Related tasks

- [Linux-UNIX: Configure S-TAP with guard-config-update](#)

Linux-UNIX: Optimizing your configuration for high load

Guardium has two options for managing a high load between the data sources and the collectors, which can be implemented individually, or together.

- [Linux-UNIX: Multi-threading S-TAP to increase S-TAP throughput](#)

S-TAP multi-threading can be used in certain workloads to prevent overrunning K-TAP buffers, and increasing the throughput of data in the S-TAP and its associated K-TAP. It works by preserving multiple threads from the point of traffic interception through to the point at which traffic is sent to the collector. You can combine multi-threading with pooled connections.

- [Linux-UNIX: Increasing S-TAP and K-TAP throughput with dynamic ring buffers](#)

By default, each sqldguard data connection is associated with one S-TAP buffer. The sqldguard thread reads data from the S-TAP buffer and sends it to collector. Enable dynamic ring buffers to add S-TAP buffers to each main sqldguard data connection, and prevent an overflow in the S-TAP buffer during traffic peaks.

Linux-UNIX: Multi-threading S-TAP to increase S-TAP throughput

S-TAP multi-threading can be used in certain workloads to prevent overrunning K-TAP buffers, and increasing the throughput of data in the S-TAP and its associated K-TAP. It works by preserving multiple threads from the point of traffic interception through to the point at which traffic is sent to the collector. You can combine multi-

threading with pooled connections.

If the K-TAP is dropping a lot of traffic, or if there is evidence that intercepting the traffic is impacting the database performance, then you might consider enabling multiple K-TAP buffer support. An increased number of S-TAP threads and K-TAP buffers may mean that there is reduced lock contention in K-TAP, and the S-TAP has an improved ability to relay traffic to the collectors. But it also means that S-TAP might use more CPU and more memory, and more memory is pinned by K-TAP.

With multi-threading, the S-TAP creates extra threads, and the K-TAP creates additional buffers to store collected data. The K-TAP balances the traffic between the buffers, placing entire packets for a single session in one buffer. Each S-TAP thread reads from a different K-TAP buffer, and sends traffic data to a single Guardium® system. The higher the number of Guardium connections, the higher the throughput. This increases the CPU usage, but it should not be significant.

Pooled connections are clustered onto a main connection and are primarily intended for helping absorb the time cost of encryption by expending more CPU cycles. With pooled connections, a separate thread (the aux thread) pulls traffic from the main connection buffer queue and sends it to the collector to which the main connection thread is connected. Pooled connections are useful even when `participate_in_load_balancing=0`, whereas extra [SQLGuard_n] sections (or `num_main_thread > 1`) at that setting are for failover only.

There are no definitive rules, you first modify the configuration, then fine-tune the results. Each database has a maximum of 50 connections to its collectors. The maximum per collector is 10, which can be 10 pooled connections, or 10 main threads, or a combination.

Multi-threading does not rectify a slow or busy network.

When one or more Guardium systems can not be reached, a failover mechanism redirects the traffic from one Guardium system to another.

Multi-threading is also supported on AIX WPARs and Solaris zones.

Look at the K-TAP buffer statistics, if you see drops, you can increase the size of the buffer or you can increase the number of buffers. If throughput is your problem, you need to increase the number of buffers. If you are concerned about a measured DB impact, increase the number of buffers. If everything looks like it's usually fine but periodically you incur drops due to specific tasks, then just increase the buffer size.

Limitations

- Encrypted and unencrypted A-TAP traffic cannot be sent to the same Guardium system, for all databases, since not all database encrypted K-TAP traffic and unencrypted A-TAP traffic can share the same session.
- Policies have to be the same on all Guardium system because the policies dictate what happens to a system's traffic. If the policies are different, there's no guarantee which policy is in effect on a given session.
- `participate_in_load_balancing` values 1 and 4 are similar but they use different mechanisms to split the traffic, so the traffic from one session might get sent to multiple collectors. If you are using 1 and switch to 4, any sessions that are currently open might move to different Guardium systems, and you could lose the session information. Sessions closed before or opened after the transition are not affected.

Configuration Guidelines

The parameter `num_main_thread` in each [SQLGuard_n] section of the `guard_tap.ini` file determines the number of main connections to each collector. The maximum value of `num_main_thread` is 10 for all of the defined Guardium hosts (all of the [SQLGuard_n] sections of the `guard_tap.ini` file). The actual number of K-TAP buffers is determined automatically, depending on the total of the `num_main_thread` for all collectors of the S-TAP. The maximum number of K-TAP buffers is five. They are automatically allocated across the read threads.:

- 1-5: one S-TAP read thread for each K-TAP buffer, and one main connection to the collector.
- 6-10: one or two S-TAP read threads for each K-TAP buffer, and one or two main connections to the collector.

The maximum value of `num_main_thread` is 10 for all of the defined Guardium hosts.

Adding collectors to implement multi-threading

In the `guard_tap.ini` file:

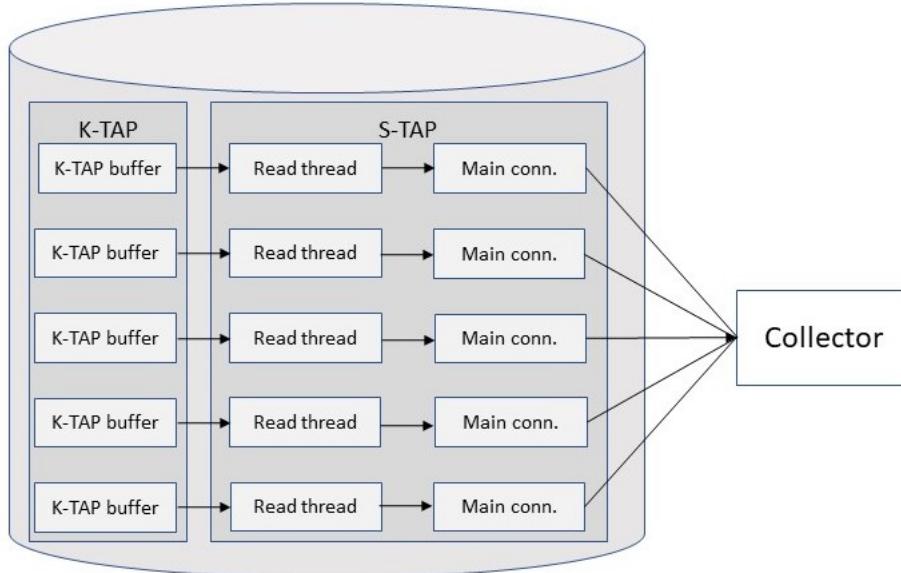
- Set `participate_in_load_balancing=4`
- Add an [SQLGuard_n] section for each added collector
- Set `num_main_thread` in all [SQLGuard_n] sections, up to a total of 10 for all collectors

Adding read threads to an under-utilized collector to implement multi-threading

If you have a relatively strong and lightly loaded collector, set or increase the `num_main_thread` parameter in the corresponding [SQLGuard_n] section.

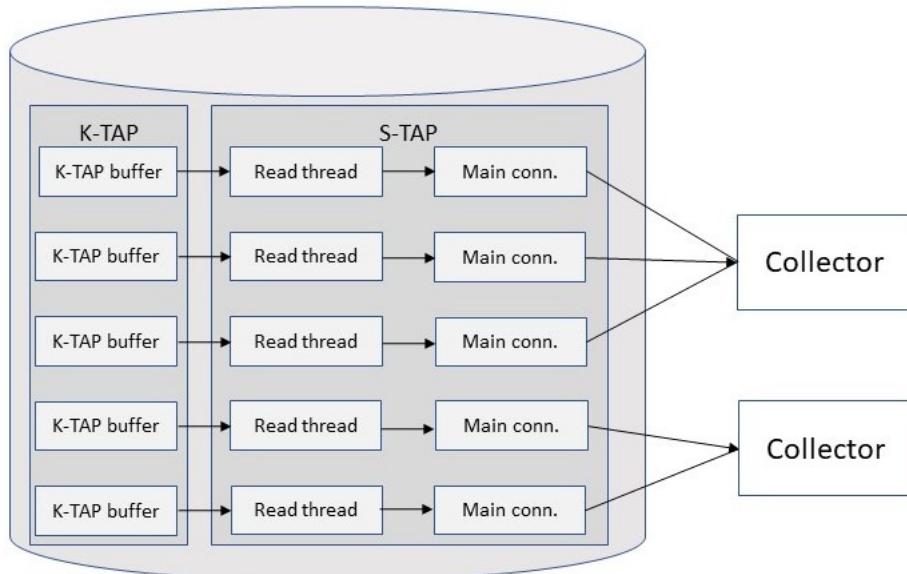
Example: One collector, five threads

```
[TAP]
...
participate_in_load_balancing=4
[SQLGuard_0]
num_main_thread=5
primary=1
```



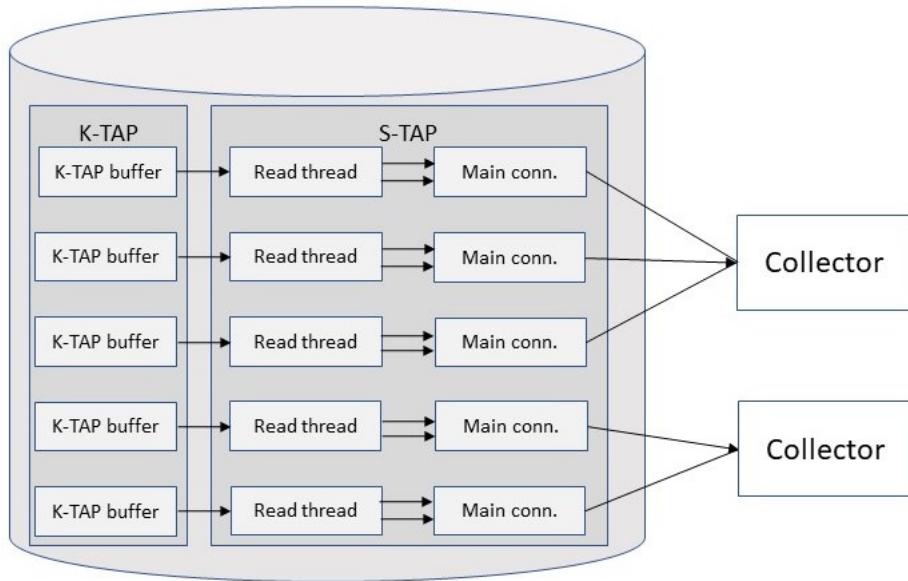
Example: Two collectors, five threads

```
[TAP]
...
participate_in_load_balancing=4
[SQLGuard_0]
num_main_thread=3
primary=1
[SQLGuard_1]
num_main_thread=2
primary=2
```



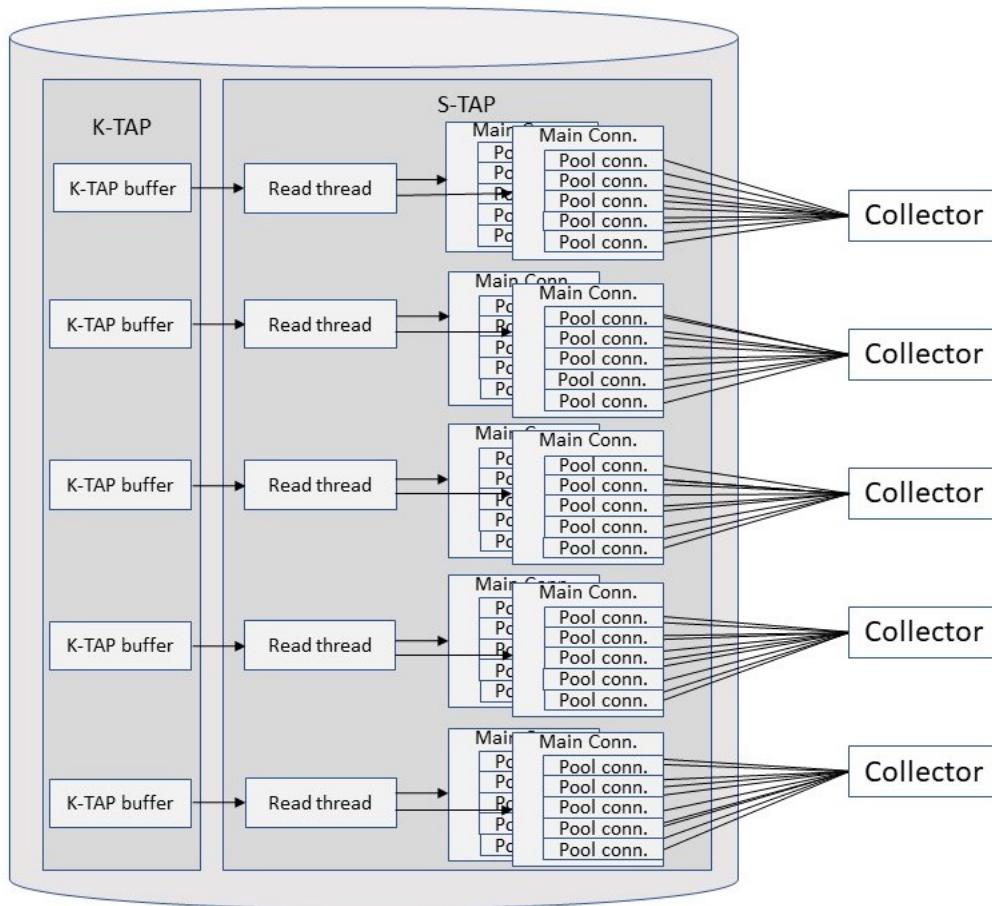
Example: Two collectors, 10 threads

```
[TAP]
...
participate_in_load_balancing=4
[SQLGuard_0]
num_main_thread=5
primary=1
[SQLGuard_1]
num_main_thread=5
primary=2
```



Example: Five collectors, 10 threads, two main connections/collector, 5 pooled threads/main connection

```
[TAP]
...
participate_in_load_balancing=4
[SQLGuard_0]
connection_pool_size=10
num_main_thread=2
primary=1
[SQLGuard_1]
connection_pool_size=10
num_main_thread=2
primary=2
...
[SQLGuard_4]
connection_pool_size=10
num_main_thread=2
primary=5
```



Related concepts

- [Linux-UNIX: S-TAP statistics](#)

Linux-UNIX: Increasing S-TAP and K-TAP throughput with dynamic ring buffers

By default, each sqlguard data connection is associated with one S-TAP buffer. The sqlguard thread reads data from the S-TAP buffer and sends it to collector. Enable dynamic ring buffers to add S-TAP buffers to each main sqlguard data connection, and prevent an overflow in the S-TAP buffer during traffic peaks.

About this task

When a ring buffer becomes full, Guardium allocates a new buffer, and all data that is captured from the K-TAP is written to the newly created buffer. The sqlguard thread always reads from the first created buffer and sends data to sqlguard. When a buffer is empty and another ring buffer is already created, the empty buffer is deleted. Guardium manages the dynamic ring buffers without user intervention: when, and how many, ring buffers to allocate, or close, per main connection. The maximum number of ring buffers is 10. If the S-TAP fails over, data in all buffers is moved to the new buffers.

Procedure

- Enable Dynamic ring buffers in the UI. For more information, see [Linux-UNIX: Configuring S-TAP in the S-TAP Control page](#).
 - Change the following parameters value to 1 in the `guard_tap.ini` file.
 - `enable_dynamic_ring_buffers`
 - 12.1 and later `enable_ktap_dynamic_ring_buffers`
- For more information, see [Linux-UNIX: General parameters](#).
- Change the following parameters in GIM.
 - `gim_enable_dynamic_ring_buffers`
 - 12.1 and later `STAP_ENABLE_KTAP_DYNAMIC_RING_BUFFERS`
- For more information, see [Set up by Client](#).

Linux-UNIX: Alerts on uninstalled S-TAPs

Uninstalling an S-TAP might be evidence of harmful activity. The predefined S-TAP Uninstall Alert notifies when an S-TAP is uninstalled. You can view the S-TAP Uninstall Events report in My Dashboards.

By default the alert is scheduled hourly. View and optionally configure the Alert Receivers in the Alert Builder: Protect > Database Intrusion Detection > Alert Builder. Tip: Best practice is to leave the alert settings at their defaults. If you need to change the configuration, run the CLI command **restart gui** so that the changes take effect. The alert writes to SYSLOG in the format: Alert Name: STAP Uninstall Alert. Alert Description: STAP Uninstall Alert... ...<S-TAP host>. The S-TAP host uniquely identifies the S-TAP. It is usually the database IP.

Related concepts

- [Predefined alerts](#)

Linux-UNIX: Deleting inactive S-TAPs in a centralized environment

You can use a cron job on the central manager to delete all inactive S-TAP instances.

Procedure

1. Go to Manage > System View > Enterprise S-TAP View.
2. In the Actions menu, select Add API mapping.
3. In the Add API Mapping dialog, search for and select **delete_inactive_stap**.
4. In the Enterprise S-TAP view, right-click in any row and select Invoke > **delete_inactive_stap**.
5. Create a script to schedule running this API periodically on the central manager.

Sample shell script for running the API:

```
#!/bin/bash

echo >> ${GUARD_LOG_DIR}/delete_inactive_staps.log
echo >> ${GUARD_LOG_DIR}/delete_inactive_staps.log

echo Deleting inactive staps from all managed units $dateStr >> ${GUARD_LOG_DIR}/delete_inactive_staps.log
date >> ${GUARD_LOG_DIR}/delete_inactive_staps.log

#Run the delete inactive stap command from CM for all S-TAPs on all managed_units

echo -e "grdapi delete_inactive_stap stapHost=all api_target_host=all_managed" | su - cli >>
${GUARD_LOG_DIR}/delete_inactive_staps.log

exit 0
```

6. Create a cron job to run the script after the report is refreshed, at whatever interval you decide for both the report refresh and the cron job.

Related reference

- [delete_inactive_stap](#)

Linux-UNIX: Monitoring S-TAP in the GUI

Use these standard reports and views to monitor your S-TAP status in the GUI.

You can create alerts that are based on exceptions that are created by S-TAPs, but other domains that are used by S-TAP reports are system-private and cannot be accessed by users.

System View

S-TAP Status Monitor in the System Monitor window: For each S-TAP reporting to this Guardium® system, this report identifies the S-TAP Host, S-TAP Version, DB Server Type, Status (active or inactive), Last Response Received (date and time), Instance Name, Primary Host Name, and true/false indicators for: K-TAP, MS SQL Server Shared Memory, DB2® Shared Memory, Win TCP, Local TCP monitoring, Named Pipes Usage, Encryption, Firewall, DB install Dir, DB port Min and DB Port Max.

Click any line to view the inspection engines that are configured for this S-TAP. The bread crumbs show where you are; click ALL S-TAPs to return to the list of S-TAP. For more details, see [Linux-UNIX: Inspection engine verification](#).

S-TAP Status Monitor: For each S-TAP reporting to this Guardium system, this report identifies the S-TAP Host, DB Server Type, S-TAP Version, Status (active or inactive), Inspection Engine status, Last Response Received (date and time), Primary Host Name, and true/false indicators for: Firewall and Encrypted. Click the S-TAP Status and the Inspection Engine status to see the Verification status on all Inspection Engines.

S-TAP Events: For each S-TAP reporting to this Guardium system, this report identifies the S-TAP Host, Timestamp, Event type (Success, Error Type, and so on), and Tap Message.

If no messages display in the S-TAP Events panel, the production of event messages may have been disabled in the configuration file for that S-TAP. If this is the case, you may be able to locate S-TAP event messages on the host system in the syslog file.

Tap Monitor

S-TAP Configuration Change History: This report is displayed only when an inspection engine is added or changed. Lists S-TAP configuration changes – each inspection engine change is displayed on a separate row. Each row lists the S-TAP Host, DB Server Type, DB Port From, DB Port To, DB Client IP, DB Client Mask, and Timestamp for the change.

Primary Guardium Host Change Log: Log of primary host changes for S-TAPs. The primary host is the Guardium system to which the S-TAP sends data. Each line of the report lists the S-TAP Host, Guardium Host Name, Period Start, and Period End.

S-TAP Status: Displays status information about each inspection engine that is defined on each S-TAP Host. This report does not have From and To date parameters, since it is reporting current status. Each row of the report lists the S-TAP Host, DB Server Type, Status, Last Response, Primary Host Name, Yes/No indicators for the following attributes: K-TAP Installed, Shared Memory Driver Installed, Db2 Shared Memory Driver Installed, Named Pipes Driver Installed, and App Server Installed. In addition, it lists the Hunter DBS.

Inactive S-TAPs Since: Lists all inactive S-TAPs that are defined on the system. It has a single runtime parameter: QUERY_FROM_DATE, which is set to now -1 hour by default. Use this parameter to control how you want to define *inactive*. This report contains the same columns of data as the S-TAP Status report, with the addition of a count for each row of the report.

Linux-UNIX: S-TAP logs

The UNIX S-TAP has a few log files.

- guard_stap* logs, located in the filepath specified by the tap_log_dir parameter.
 - guard_stap.stderr.txt: contains all the output (and the extra debugging output) of S-TAP
 - guard_stap.fam.txt: Exists only if FAM is enabled; contains all the output (and extra debug) of FAM monitoring.
 - guard_stap.stdout.txt: Since v10.1.4, it is present in the system, but not used.
- UNIX system log (/var/adm/syslog, /var/log/messages, name and location as relevant on the particular system): contains K-TAP module output messages (along with output messages from all other kernel tasks).

Linux-UNIX: Viewing S-TAP debug details on the database

You can view some S-TAP debug details on the database itself, by using the .stap_state file, located in the S-TAP installation directory.

About this task

Procedure

In the S-TAP installation directory of the database, enter (by default):

```
[root@<server> ~]# /usr/local/guardium/guard_stap/stap_state_ctl /usr/local/guardium/guard_stap/.stap_state
```

Typical output:

```
Stap State:  
filename: /usr/local/guardium/guard_stap/.stap_state  
version: 1  
pid: 73347  
process_start: 1600771074  
debug_level: 0  
ticker: 619  
proxy_keys_req_sent_at: 0  
proxy_send_keys_req: 0  
proxy_send_cert_sign_req: 0  
proxy_keys_awaiting_resp: 0  
proxy_transit_key_req_sent_at: 0  
proxy_send_transit_key_req: 0  
proxy_transit_key_awaiting_resp: 0  
proxy_error_pending: 0  
pushed_keys_to_gproxyd: 0  
exit_interface_ready: 0  
[root@<server> ~]#
```

Linux-UNIX: Determine the S-TAP version

Procedure

1. From the GUI, the S-TAP version number is displayed in Manage > System View > S-TAP Status Monitor
2. Alternatively, you can display the S-TAP version number from the UNIX command line of the database server, by running the guard_stap binary with the -version or --version argument

For example, assuming the S-TAP is installed in the default installation directory, enter one of these commands:

```
-bash-3.2# <guardium_base>/modules/STAP/current/guard_stap --version
```

```
-bash-3.2# <guardium_base>/guard_stap/guard_stap --version  
STAP-doberman_r20511_1-20100728_0514
```

Linux-UNIX: S-TAP statistics

S-TAP statistics are easily viewed in the predefined S-TAP and External S-TAP Statistics report.

You can create alerts based on results.

S-TAP statistics collection is configured with the parameter `stap_statistic`. This is an advanced parameter and should be modified only by Guardium Technical Support or advanced users. It specifies the interval at which the S-TAP sends statistics to the sniffer. Valid values are:

- Positive integer: for hours
- Negative integer: minutes
- 0: do not send

Some statistics are cumulative and some are real time. Cumulative fields require reset to get the current count. Real-time fields are dynamic and do not require a reset. The values can be reset directly from the database server only, by running the following command:

```
<S-TAP Shell Install Directory>/guard_stap/ktap/current/guard_ktap_stat reset
```

or

```
<S-TAP GIM Install Directory>/modules/KTAP/current/guard_ktap_stat reset
```

Cumulative fields are indicated as such in the following lists.

- CPU statistics**
- `system_cpu_percent`
- Shows the overall CPU usage of S-TAP for the entire system. It is calculated by using the `pcpu` option from the `ps` command. These situations might indicate a problem:
- Usage is consistently at, or near, 100%. Such a condition might indicate that the `guard_stap` process is stuck in a loop and is using all of the resources on one core. Run the `guard_diag` command when you encounter such cases.
 - Overall usage is abnormally high. This number depends on the total number of cores that are running on the system. For example, consider a consistent S-TAP CPU usage of 5% on a system with 16 cores. In this case, 5% indicates that S-TAP is consistently using 80% of one core. If S-TAP is consistently running that high, it leaves little overhead to accommodate any other spikes in traffic. Worse, S-TAPs that are running close to 100% of one core might introduce performance degradation on the host server because it can make S-TAP unresponsive to K-TAP requests.
- `system_cpu_idle_percent`
- Total system CPU free.
- `stap_cpu_percent`
- Average system CPU usage of S-TAP over life of process. This statistic shows how busy the host server is overall. For example, if the system has 10 cores, and S-TAP is using 30% of one, the overall S-TAP CPU usage is about 3%. The maximum CPU an S-TAP can use depends on the threading. See [Linux-UNIX: Multi-threading S-TAP to increase S-TAP throughput](#).
- `buffer_recycled`
- Cumulative. Recycle count for this index S-TAP buffer.
- Indicates the number of times the S-TAP buffer overflowed, which is highly indicative of S-TAP performance issues on the host server. The S-TAP buffer can overflow for several reasons, including:
- Insufficient network bandwidth to accommodate the volume of data that is sent by the S-TAP to the Guardium appliance. This issue is most prevalent when the Guardium appliance and host database server are not in the same data center or LAN.
 - Guardium collector is too busy to handle the volume that is sent from S-TAP (this is a rare case).
- `timestamp`
- Time at which the record was created.
- `software_tap_host`
- The host system where data is collected. (`tap_ip` value in the S-TAP configuration.)
- The reset command resets all of the K-TAP statistics.
- K-TAP statistics**
- `timestamp`
- Time at which the record was created.
- `software_tap_host`
- The host system where data is collected. (`tap_ip` value in the S-TAP configuration.)
- `ktap_buffer_index`
- The K-TAP buffer that this cluster of parameters refers to (mostly).
- `total_bytes_so_far`
- The total number of bytes that were processed by K-TAP since the last reset of these values. Reset the counters to come to any meaningful conclusions with this data.
- This counter rolls back over to 0 after it reaches 4294967296 bytes (2^{32}). If the last reset was a while back, the counter might be a value that was rolled over several times. On its own, there is little that can be learned from looking at only the total bytes processed value. Its delta over time can be used to estimate the volume of traffic that is processed by S-TAP if K-TAP is the only driver that is used to intercept traffic. For this purpose, it is not necessary to first reset the counter. Total Bytes Processed is most helpful when it is used as baseline for some of the other statistics that are described next.
- `total_bytes_dropped_so_far`
- Cumulative. The total number of bytes that were dropped by K-TAP since the last reset of these values. Reset the counters to come to any meaningful conclusions with this data.
- By default, K-TAP uses a 4 MB buffer file, which is configurable from the `guard_tap.ini`. If the `guard_stap` process cannot read data quickly enough from this buffer, K-TAP starts dropping data and the drops are reflected in this field. The significance of any drops that are shown here should be put in the context of Total Bytes Processed so Far. An excessive number of bytes dropped can be indicative of issues, including: Insufficient resources on host server for S-TAP (`guard_stap` process) to read data from the K-TAP buffer in a timely manner.
- `total_bytes_ignored`
- Cumulative. The amount of database traffic that is ignored at the K-TAP level when IGNORE STAP SESSION rules are implemented in the Guardium policy, since the last reset of these values. It is useful for estimating how effectively the policy is ignoring traffic. Total Bytes Ignored should be considered only after a reset and in the context of Total Bytes Processed so Far.
- `total_buffer_init`
- Cumulative. The number of times the K-TAP buffer was reinitialized. S-TAP can reinitialize the K-TAP buffer if any corruption of buffered data is detected.

ioctl_requests
Cumulative. Number of K-TAP requests issued so far (not per buffer).

total_response_bytes_ignored
Cumulative. The bytes of database response traffic that is ignored at the K-TAP level as the result of any IGNORE RESPONSES PER SESSION rules that are implemented in the Guardium policy, since the last reset of these values.

total_packet_count
Number of packets seen since the last reset of these values.

time_since_last_reset_in_seconds
Time that is elapsed since last statistics reset.

CPU statistics

system_cpu_percent
Shows the overall CPU usage of S-TAP for the entire system. It is calculated by using the pcpu option from the ps command. These situations might indicate a problem:

- Usage is consistently at, or near, 100%. Such a condition might indicate that the guard_stap process is stuck in a loop and is using all of the resources on one core. Run the **guard_diag** command when you encounter such cases.
- Overall usage is abnormally high. This number depends on the total number of cores that are running on the system. For example, consider a consistent S-TAP CPU usage of 5% on a system with 16 cores. In this case, 5% indicates that S-TAP is consistently using 80% of one core. If S-TAP is consistently running that high, it leaves little overhead to accommodate any other spikes in traffic. Worse, S-TAPs that are running close to 100% of one core might introduce performance degradation on the host server because it can make S-TAP unresponsive to K-TAP requests.

system_cpu_idle_percent
Total system CPU free.

stap_cpu_percent
Average system CPU usage of S-TAP over life of process. This statistic shows how busy the host server is overall. For example, if the system has 10 cores, and S-TAP is using 30% of one, the overall S-TAP CPU usage is about 3%. The maximum CPU an S-TAP can use depends on the threading. See [Linux-UNIX: Multi-threading S-TAP to increase S-TAP throughput](#).

Buffer statistics

stap_buffer_usage_percent
Average percentage use of all S-TAP buffers.

buffer_recycled
Cumulative. Recycle count for this index S-TAP buffer.
Indicates the number of times the S-TAP buffer overflowed, which is highly indicative of S-TAP performance issues on the host server. The S-TAP buffer can overflow for several reasons, including:

- Insufficient network bandwidth to accommodate the volume of data that is sent by the S-TAP to the Guardium appliance. This issue is most prevalent when the Guardium appliance and host database server are not in the same data center or LAN.
- Guardium collector is too busy to handle the volume that is sent from S-TAP (this is a rare case).

A-TAP statistics

activated_ataps
Comma-separated list of instance names that are active.

non_activated_ataps
Comma-separated list of instance names that are inactive.

erroneous_ataps
Comma-separated list of instance names that states that appear to be improper.

dropped_priority_packets
Count of priority packets that were dropped.

Shared memory statistics

exit_number_of_shmem_segments
Total number of shmem segments.

exit_total_packets_so_far
Total packet count seen by this shm region.

exit_total_bytes_so_far
Total packet byte count seen by this shm region.

exit_total_0_16_bytes_packets
Total packet count seen where packet size > 0 && <= 16.

exit_total_16_4k_bytes_packets
Total packet count seen where packet size > 16 && <= 4000.

exit_total_4k_16k_bytes_packets
Total packet count seen where packet size > 4000 && <= 16000.

exit_total_16k_32k_bytes_packets
Total packet count seen where packet size > 16000 && <= 32000.

exit_total_32k_plus_bytes_packets
Total packet count seen where packet size > 32000.

exit_total_bytes_dropped_so_far
Total number of bytes dropped.

exit_total_packet_drops_so_far
Total number of packets dropped.

Proxy statistics

proxy_active_ssl_connections
Number of active SSL sessions through proxy.

proxy_memory_usage
Memory (in KB) that proxy is using.

proxy_cpu_usage
Amount of cpu (percentage) that proxy is using.

proxy_latency_0ms_1ms
count of packets with latency 0-1ms.

```

proxy_latency_1ms_10ms
    count of packets with latency 1ms-10ms.
proxy_latency_10ms_100ms
    Count of packets with latency 10ms-100ms.
proxy_latency_100ms_1s
    Count of packets with latency 100ms-1s.
proxy_latency_1s_plus
    Count of packets with latency greater than 1s.
proxy_last_minute_tcp_payload
    Amount of tcp data (in bytes) handled by proxy in last minute.
proxy_last_minute_tls_payload
    Amount of TLS data (in bytes) handled by proxy in last minute.
proxy_last_minute_total_connections
    Total number of connections accepted by proxy in last minute.
proxy_last_minute_ssl_accepted_connections
    Total number of SSL connections accepted by proxy in last minute.

```

S-TAP buffer statistics

```

stap_total_packets_dropped
    Total number of packets dropped due to insufficient buffer space in the S-TAP service.
stap_total_bytes_dropped
    Total number of bytes dropped due to insufficient buffer space in the S-TAP service.
stap_collector_count
    Number of collectors.
stap_collector_names
    Comma-delimited list of all the collectors that are assigned to the S-TAP.
stap_collector_packets_dropped
    Comma-delimited list of collector packet drop count, in the same order as stap_collector_names.
stap_collector_bytes_dropped
    Comma-delimited list of collector byte drop count, in the same order as stap_collector_names.

```

Linux-UNIX: S-TAP Monitor (`guard_monitor`)

The S-TAP Watchdog (`guard_monitor`) monitors S-TAP performance and responsiveness. You can configure specific actions that are triggered when the S-TAP exceeds certain thresholds.

Note: On HP-UX 11.11, the information about the process command is limited to 64-characters. This means that if the full path to the `guard_stap` binary is longer than 64-characters, the Guardium monitor cannot recognize it.

Monitoring covers:

- CPU utilization: checked with the `ps` command or using cpu time from `procfs`
- CPU responsiveness to polling: checked by sending the S-TAP process a console request and waiting for a response.

If S-TAP CPU utilization exceeds the configured threshold, or if S-TAP does not respond to the console request, the following actions can be taken:

- Automatically run `guard_diag`.
- Automatically kill the S-TAP process.
- Automatically core dump and kill the S-TAP process.
- Automatically trace S-TAP process.

Guard Monitor installs automatically at the end of the S-TAP installation. There are no user prompts and no install progress is shown. During S-TAP uninstall, Guard Monitor is automatically uninstalled. The user no longer has the option to reboot in the installer and is instead just notified that a reboot is necessary to complete the uninstall. This reboot is not critical but it is necessary if the user intends to install S-TAP again on the system. If the user uninstalls, does not reboot, and then tries to reinstall there will be an popup blocking the installation notifying the user that S-TAP is partially installed and the server needs to be rebooted.

The `guard_monitor` runs with its configuration file, `guard_monitor.ini` as its argument. The monitor is controlled by using the `guard_monitor.ini` file. For Shell installations, you can make all configuration changes directly on the configuration file. For GIM, use the interface in the GUI to make any changes.

Guard_monitor is not enabled by default. In shell installations, enable it from `initab` by uncommenting the “`umon`” line, or by using the services control facility for the particular Operating Systems (`initctl` for RedHat 6, `systemctl` for RedHat 7, `SMF` for Solaris 10 and up). For GIM installations, `guard_monitor` is enabled by setting `STAP_UTILS_START_MONITOR=y`.

Note: `guard_monitor` requires administrative privileges (root).

The default location for the S-TAP Monitor output is `/var/tmp/monitor`. This location can be configured from `guard_monitor.ini` (configuration file). See the example of the `guard_monitor.ini` file at end of this topic.

After enabling `guard_monitor`, make sure the process is running on the database server.

Examples of settings

Default thresholds are provided for each function. For example, you might want to monitor CPU usage, and set one threshold (75%) for gathering diagnostic information and a higher threshold (85%) at which the S-TAP is killed. You would set `auto_diag=1` to enable gathering of diagnostic information, and `diag_high_cpu_level=7500` to gather diagnostic information when CPU usage reaches 75%. Then set `auto_kill_on_cpu_enable=1` to enable automatic killing of the S-TAP process, and set `auto_kill_on_cpu_level=8500` to kill the process when CPU usage reaches 85%.

But you may not want to keep killing the S-TAP process repeatedly, so you can set a limit on that as well. You can limit how many times the process can be killed within one hour by setting `kill_num_in_hour=5`. Then specify what should happen when the limit is reached: code `final_action=1` to disable the S-TAP, or `final_action=2` to allow it to continue running.

Guard_monitor CPU polling parameters

| guard_monitor.ini | GIM | Description | Default |
|---------------------------|---|--|----------------|
| poll_cpu_interval | STAP-
UTILS_MONITOR_POLL_CPU_INTERVAL | Interval, in seconds, at which guard_monitor checks S-TAP CPU utilization. When checking CPU utilization, guard_monitor measures the average CPU utilization over the life of the guard_stap process using <i>ps</i> . This means that S-TAP has to run above the CPU threshold for some time before guard_monitor detects a problem. | 10 |
| cpu_measurement_timeslice | | Interval over which CPU consumption is measured, in seconds. | 0 |
| poll_stap_interval | STAP-
UTILS_MONITOR_POLL_STAP_INTERVAL | Interval at which guard_monitor sends a console S-TAP request, in seconds. | 10 |
| cpu_measurement_mode | NA | <p>Method for calculating CPU consumption:</p> <ul style="list-style-type: none"> • 0: measure single CPU consumption • 1: measure average CPU consumption across all CPU capacity of Guardium system; total CPU consumption/number of CPUs. <p>When cpu_measurement_mode=1 and cpu_measurement_timeslice=0, only one CPU usage is measured.</p> | 0 |
| nonresponsive_action | NULL | Action taken when S-TAP does not respond to polls. <ul style="list-style-type: none"> • diags • trace • NULL | |

Monitoring actions

| guard_monitor.ini | GIM | Description | Default |
|--------------------------|--|--|--|
| logs_to_rotate | STAP-
UTILS_MONITOR_LOGS_TO_ROTATE - | Logs to be rotated | /tmp/guard_stap.stderr.txt,/tmp/guard_stap.stdout.txt,/usr/local/guardium/guard_stap/ktap/ktap_install.log,/usr/local/guardium/guard_stap/guard_discovery.stderr.log |
| log_rotate_size | STAP-
UTILS_MONITOR_LOG_ROTATE_SIZE | Maximum file size of monitor log file, in KB. (Log files are rotated when they reach this size.) | 1024 |
| log_rotate_num_kept | STAP-
UTILS_MONITOR_LOG_ROTATE_NUM_KEEP | The number of rotated monitor logs on disk. | 5 |

Auto-Diag action

If S-TAP CPU utilization exceeds the configured threshold, the most basic action guard_monitor takes is an automatic guard_diag.

By default, the output from the guard_diag is placed in /var/tmp. The file name is derived from the machine name, and the time/date run; it always starts with diag.ustap.

| guard_monitor.ini | GIM | Description | Default |
|--------------------------|--|---|----------------|
| auto_diag | STAP-
UTILS_MONITOR_AUTO_DIAG | Enables automatic guard_diag. 0=no, 1=yes. | 1 |
| diag_high_cpu_level | STAP-
UTILS_MONITOR_DIAG_HIGH_CPU_LEVEL | The S-TAP CPU threshold at which guard_monitor initiates a guard_diag. Enter (%CPU threshold*100). v10.1.4 and higher: When cpu_measurement_mode=1, the % can be higher than 100. | 7500 |
| diag_num | STAP-
UTILS_MONITOR_DIAG_NUM | Enables creation of more than one guard_diag output. Integer. | 2 |

Auto-Kill action

Use these parameters to configure the S-TAP auto-kill.

| guard_monitor.ini | GIM | Description | Default |
|--------------------------|--|--|----------------|
| auto_kill_on_cpu_enable | STAP-
UTILS_MONITOR_AUTO_KILL_ON_CPU_ENABLE | Enable automatic S-TAP kill. 0=no, 1=yes. | |
| auto_kill_on_cpu_level | STAP-
UTILS_MONITOR_AUTO_KILL_ON_CPU_LEVEL | The S-TAP CPU threshold at which guard_monitor kills S-TAP. Enter (%CPU threshold*100). v10.1.4 and higher: When cpu_measurement_mode=1, the % can be higher than 100. | 8500 |
| kill_num_in_hour | STAP-
UTILS_MONITOR_KILL_NUM_IN_HOUR | The maximum number of times guard_monitor is killed in an hour. Integer value. | 5 |
| final_action | STAP-
UTILS_MONITOR_FINAL_ACTION | Action taken when max kills per hour is reached. <ul style="list-style-type: none"> • 1 = Disable S-TAP. • 2 = Stop killing S-TAP and let it continue. | |

Core dump S-TAP before kill

Some S-TAP issues, such as when S-TAP gets stuck in a loop, require more information than provided in the guard_diag output.

The guard_monitor performs automatic core dumping of the S-TAP process. The guard_monitor core dumps S-TAP before killing the process (if S-TAP auto kill is enabled).

Location of core dumps created by guard_monitor: /var/tmp/monitor/coredumps

These parameters configure auto core dumps:

| guard_monitor.ini | Description | Default |
|------------------------|---|---------|
| force_core_before_kill | The type of core dump to generate:
sigsegv: This is the most portable of the options, but requires the SA to configure ulimit to enable core dumping.
gcore: The most useful, but requires gcore to be installed on the system. Linux platforms only.
pstack: Least useful of the options, but may be the only utility available on certain systems. Linux platforms only.
NULL: disabled | |
| force_core_when | When to collect a core dump:
limitexceeded: collect core when S-TAP is killed due to exceeding a resource limit
nonresponsive: collect core when S-TAP is killed due to it being nonresponsive
always: always collect core | always |
| kill_oldcore_saved | Integer. Specifies whether generated core dumps are saved. When set to non-zero, guard_diag keeps all core dumps generated. Otherwise, it deletes the old core dumps each time a new one is generated. | |

Example of guard_monitor.ini

```
The following section header is required for GIM to recognize this .ini file.
; otherwise, it serves no purpose

[TAP]
; output dir for monitor logs, diags, traces, etc.
monitor_output_dir=/var/tmp
; location of guardium installation (need not be where monitor is installed, for example, /usr/local)
stap_dir=/usr/local
; ip to connect to for downloading configuration file and uploading diags and trace output
; this is parsed out of the guard_tap.ini, but backup value here is kept in sync
sqlguard_ip=NULL
; polling interval to verify that server end is still alive (secs)
poll_server_interval=20
; polling interval to check CPU level (secs)
poll_cpu_interval=10
; polling interval to communicate with STAP (secs)
poll_stap_interval=10
; maximum file size of monitor log file (KB)
monitor_log_rotate_size=1024
; number of rotated monitor logs to keep
monitor_log_rotate_num_kept=5
; maximum file size of log files (KB)
log_rotate_size=4096
; number of rotated logs to keep
log_rotate_num_kept=5
; logs to rotate
logs_to_rotate=/tmp/guard_stap.stderr.txt,/tmp/guard_stap.stdout.txt,/usr/local/guardium/guard_stap/ktap/ktap_install.log,
/usr/local/guardium/guard_stap/guard_discovery.stderr.log
; maximum number of STAP kills per hour (doesn't count kills resulting from auto_kill_on_intercept)
kill_num_in_hour=5
; disable STAP when kills per hour limit hit or disable kills and let STAP continue
; disable STAP: 1; disable kill: 2
final_action=2
; automatic kill STAP on CPU level on/off (1/0)
auto_kill_on_cpu_enable=0
; CPU level for kill (% * 100)
auto_kill_on_cpu_level=8500
; snif timeout for kill (secs, 0 disabled)
auto_kill_on_snif_timeout=0
; KTAP timeout for kill (secs, 0 disabled)
auto_kill_on_ktap_timeout=0
; PCAP timeout for kill (secs, 0 disabled)
auto_kill_on_pcap_timeout=0
; TEE timeout for kill (secs, 0 disabled)
auto_kill_on_tee_timeout=0
; SHMEM timeout for kill (secs, 0 disabled)
auto_kill_on_shmem_timeout=0
; automatic diags on/off (1/0)
auto_diag=1
; number of diags runs
diag_num=2
; time between diags runs (mins)
diag_interval=2
; keep old diag files or not yes/no (1/0)
diag_olddrun_saved=0
; kill STAP process after diags yes/no (1/0)
diag_auto_kill=0
; CPU level to trigger diags (% * 100)
diag_high_cpu_level=7500
; snif timeout to trigger diags (secs, 0 disabled)
diag_snif_timeout=0
```

```

; KTAP timeout to trigger diags (secs, 0 disabled)
diag_ktap_timeout=0
; PCAP timeout to trigger diags (secs, 0 disabled)
diag_pcap_timeout=0
; TEE timeout to trigger diags (secs, 0 disabled)
diag_tee_timeout=0
; SHMEM timeout to trigger diags (secs, 0 disabled)
diag_shmem_timeout=0
; automatic trace on/off (1/0)
auto_trace=0
; max time to run trace (secs)
trace_max_time=30
; max log file size for trace (MB)
trace_max_log_size=10
; keep old trace log files yes/no (1/0)
trace_oldlog_saved=0
; kill STAP when trace runs to completion yes/no (1/0)
; (e.g. is not cancelled due to low CPU)
trace_kill_on_complete=0
; CPU level to trigger trace (% * 100)
trace_high_cpu_level=6000
; low CPU level to cancel trace (% * 100)
trace_low_cpu_level=3500
; timeout for snif communication trigger (secs, 0 disabled)
trace_snif_timeout=0
; timeout for KTAP communication trigger (secs, 0 disabled)
trace_ktap_timeout=0
; PCAP timeout to trigger trace (secs, 0 disabled)
trace_pcap_timeout=0
; TEE timeout to trigger trace (secs, 0 disabled)
trace_tee_timeout=0
; SHMEM timeout to trigger trace (secs, 0 disabled)
trace_shmem_timeout=0
; auto-kill STAP when we're not intercepting databases that are configured yes/no(1/0)
; feature is also disabled when guard_tap.ini shows that STAP is running as root
auto_kill_on_intercept=0
; minimum time between STAP requested kills (mins)
intercept_min_time_interval=15
; maximum number of intercept kills per hour
intercept_max_num_in_hour=0
; number of seconds across which CPU consumption is measured (secs, 0 disabled)
; when disabled, CPU consumption is measured across the life of the process
cpu_measurement_timeslice=0
; method for calculating CPU consumption (0 or 1)
; 0: measure CPU consumption relative to one core
; 1: measure CPU consumption taking number of cores into account
cpu_measurement_mode=0
; when to collect a core dump (always, limitexceeded, nonresponsive)
; limitexceeded: collect core when STAP is killed due to exceeding a resource limit
; nonresponsive: collect core when STAP is killed due to it being nonresponsive
; always: always collect core
force_core_when=always

; STAP nonresponsive action
; run diags before killing STAP : diags
; collect trace before killing STAP: trace
; no collection, just kill STAP : NULL
nonresponsive_action=diags

```

Linux-UNIX: Troubleshooting S-TAP problems

You can use the S-TAP Status monitor tab of the System View to begin investigating any problems. Sometimes you might need to use other tools, particularly if you are monitoring databases for which the inspection engines cannot be verified.

If an S-TAP is not connected to your Guardium® system

Check whether the IBM Security Guardium S-TAP service is running on the database server:

On the database server, from the command line, run the command **ps -ef | grep stap** to verify that the S-TAP process is running. In the process list, look for /guardium/guard_stap.

Make sure that the sniffer is running on the server with the S-TAP service.

Check the communication between the sniffer and S-TAP.

For more information about possible errors, see [Table 2](#).

How to identify the S-TAP version?

- From the GUI, the S-TAP version number is displayed in Manage > System View > S-TAP Status Monitor
- Alternatively, you can display the S-TAP version number from the command line of the database server.

Run debug from the command line to quickly identify configuration issues

Use the GUI or the guard_tap.ini file to change the debug level to 4. (Other values do different things, not all of them debug). There are a few guard_stap* logs, which are located in the filepath that is specified by the tap_log_dir parameter.

- guard_stap.stderr.txt: contains all the output (and the extra debugging output) of S-TAP
- guard_stap.fam.txt: Exists only if FAM is enabled; contains all the output (and extra debug) of FAM monitoring.
- guard_stap.stdout.txt: Since v10.1.4, it is present in the system, but not used.

Verify the connection between the database server and the Guardium system

- Verify that you can ping the Guardium system at **sqlguard_ip** from the database server.

- If the ping is successful, verify that you can telnet to the following ports on the Guardium system: 16016/16018.

If there is a firewall between the database server and the Guardium system

Verify that the following ports are open for traffic between these two systems: 16016, or 16018 for encrypted connections; if you're using FAM then verify ports 16022 or 16023 for encrypted.

Note: Use the following command to check the port availability: `nmap -p port guardium hostname or IP`

Verify that the `sqlguard_ip` parameter is set to the correct guardium hostname or the IP for the Guardium system that you are connecting to.

1. Click `Manage > Activity Monitoring > S-TAP Control` to open S-TAP Control.
2. Locate the S-TAP Host for the IP address that corresponds to your database server.
3. Expand the Guardium Hosts subsection, and verify that the active Guardium Host is correctly configured.
4. If necessary, click `Modify` to update the Guardium Hosts.

Verify that the S-TAP process is not repeatedly restarting

On the database server, run the command `ps -eaf | grep stap` to verify that the process for S-TAP is not changing.

Verify that S-TAP Approval is not turned on

If S-TAP Approval is turned on, any new S-TAP that connects to the Guardium system is refused.

1. Click `Manage > Activity Monitoring > S-TAP Certification` to open S-TAP Certification.
2. Look at the S-TAP Approval Needed checkbox. If this box is checked, new S-TAPs can connect to this Guardium system only after they are added to the list of approved S-TAPs.
3. If S-TAP Approval is turned on, access the Approved Tap Clients report to view a list of approved S-TAPs. If the S-TAP that you are investigating is not on this list, return to the S-TAP Certification page, enter the IP address of the S-TAP in the Client Host field, and click `Add`.

For more information, see [Allow \(approve\) S-TAP connection to Guardium \(S-TAP certification\)](#).

If the S-TAP shows green status but no data is being processed

Check the status of the A-TAP.

Db2 shared memory traffic is not captured

Verify that the IE configuration is correct. Run the script `find_db2_shmem_parameters.sh`, located under `stap_directory/bin`. Execute it either as root or Db2 user, that uses the Db2 instance name as a parameter. It returns the shared memory parameters, including Db2 shared memory size, client position and header size. Verify that the IE parameters defined in the S-TAP match these returned values.

S-TAP verification issues

The verification process attempts to log in to your database's STAP client with an erroneous user ID and password to verify that this attempt is recognized and communicated to the Guardium system. Your S-TAP might be configured in a way that prevents the inspection engine message from reaching the Guardium system from which the request was made.

These configuration details include:

- Load balancing: if the S-TAP is configured to return responses to more than one Guardium system, the error message might be sent to a different Guardium system.
- Failover: If secondary Guardium systems are configured for the S-TAP, the error message might be sent to a secondary Guardium system if the primary Guardium system is too busy.
- `db_ignore_response`: if the S-TAP is configured to ignore all responses from the database, it does not send error messages to the Guardium system.
- Client IP/mask: if any mask is defined that is not 0.0.0.0, it might prevent the error message from being sent.
- Exclude IP/mask: if any mask is defined that is not 0.0.0.0, it might prevent the error message from being sent.

Enable FAM as S-TAP is installed with default value of `fam_installed` as 0 so the FAM does not load and is disabled.

To enable FAM, follow the applicable instructions:

For Shell installation on the database server

In the `guard_tap.ini` S-TAP configuration file, update the value of `fam_installed` and `fam_enable` parameters to 1 and then restart the server.

For GIM S-TAP bundle installation

Update the value of `STAP_FAM_INSTALLED` and `STAP_FAM_ENABLED` parameters to 1 and then restart the server.

TLS 1.3 and FIPS 140-3 not supported on Solaris operating system

IBM Security Guardium does not support Transport Layer Security (TLS) 1.3 in Guardium Data Protection version 12.0 and later on the Solaris operating system.

IBM Security Guardium does not support FIPS 140-3 cryptographic providers in Guardium Data Protection version 12.1 on the Solaris operating system.

Related topics:

- [Linux-UNIX: Monitoring S-TAP in the GUI](#)
- [Linux-UNIX: S-TAP Monitor \(guard_monitor\)](#)
- [Linux-UNIX: Inspection engine verification](#)

Db2 for IBM i S-TAP

You can use the Guardium Db2 for i S-TAP to monitor and report on any database access on IBM i. This includes any programs, such as RPG, that use native database I/O operations or SQL access.

You can use information gathered by the Guardium Db2 for i S-TAP to create activity reports, help you meet auditing requirements, and generate alerts of unauthorized activity. Detailed auditing information includes:

- Session start and end times
- TCP/IP address and port
- Object names (for example, tables or views)
- Users
- SQLSTATEs
- Job and Job numbers
- SQL statements and variables
- Client special register values

- Interface information, such as ODBC, ToolboxJDBC, Native JDBC, .NET, and so on

The S-TAP receives data from two sources:

- SQL Performance Monitor (otherwise known as database monitor) data for SQL applications
- Audit entries from the QSYS/QAUDJRN audit journal for applications using non-SQL interfaces

Data from these sources includes:

- Any SQL access whether it is initiated on the IBM i server or from a client
- Any native access that is captured in the audit journal

The S-TAP sends this data to the Guardium® system in real time.

Note: The Db2 for IBM i S-TAP supports basic S-TAP features only. Features such as blocking, query rewrite, and FAM are not supported.

For more information about the Db2 for i S-TAP and related topics, see:

- [IBM i developer overview](#)
- [IBM i on IBM Docs](#)

i S-TAP for encryption, load balancing, and failover

The IBM i S-TAP supports TLS encryption and S-TAP session load balancing/failover.

Note: i S-TAP TLS support and load balancing is supported only for IBM i 7.1 and 7.2.

Similar to UNIX S-TAPs, i S-TAP configuration parameters are saved in a `guard_tap.ini` file in the `/usr/local/guardium` directory on the IBM i server.

Administrators configure the S-TAP is done using the same APIs and UI (S-TAP Control) as other UNIX S-TAPs. When the GUI or API is used to make a change to the S-TAP configuration, the Guardium sniffer sends a message to the S-TAP, which backs up the old `.ini` file, saves the configuration to the new `.ini` file and then restarts itself.

Administrators can set up encrypted communication between the S-TAP and the appliance using the S-TAP configuration controls as well as set up various load balancing options.

Using S-TAP failover and load balancing

The failover and load balancing options for the i S-TAP are similar to what exists for UNIX S-TAPs. Use the `participate_in_load_balancing` parameter to determine whether to use failover or load balancing behavior, and use the SQLGuard sections of your S-TAP to set up primary, secondary, and tertiary Guardium hosts.

One difference is that there is no need for `participate_in_load_balancing=3`; because of the way the I S-TAP communication is architected, complete session information is available on each message. This means that even before the enhancements delivered in this patch, you could have used hardware balancing (such as F5) with `participate_in_load_balancing=1` and a virtual IP address in the primary SQLGuard section of the configuration file.

In a failover configuration, the S-TAP is configured to register with multiple collectors, but only send traffic to one collector at a time (`participate_in_load_balancing=0`). The S-TAP in this configuration sends all its traffic to one collector unless it encounters connectivity issues to that collector that triggers a failover to a secondary collector.

How to use AppEvent from IMS

The data holding user information of an APP_EVENT DLI call needs to have similar syntax as GuardAppEvent api.

The first two bytes represent ccsid of the encoding of the following bytes. For example, 0x04B8 stands for ccsid 1208. The following bytes need to have the syntax as below:

SELECT

```
'GuardAppEvent:Start',
'GuardAppEventType:type',
'GuardAppEventUserName:name',
'GuardAppEventStrValue:string',
'GuardAppEventNumValue:number',
'GuardAppEventDateValue:date'
```

FROM DUAL

For further reference for type, name, string, number, date, check GuardAppEvent API.

Currently, only UTF8 encoding is supported.

- [Monitoring strategy](#)

Make your monitoring and auditing effective and efficient by developing a strategy that recognizes and fulfills your regulatory and other requirements.

- [Installing the S-TAP for IBM i](#)

The S-TAP software is a shell script that you must run from IBM i, within the Portable App Solutions Environment (PASE) environment. Take the following steps to upload the S-TAP software to the IBM i Integrated File System (IFS) and then install it.

- [Uninstalling the S-TAP](#)

- [Upgrading the S-TAP from 10.x to 11.x for IBM i](#)

- [Defining the S-TAP for IBM i](#)

After you install the S-TAP, ensure that it can communicate with the Guardium system.

Monitoring strategy

Make your monitoring and auditing effective and efficient by developing a strategy that recognizes and fulfills your regulatory and other requirements.

After you know what data you need, develop a strategy for collecting it with as little extraneous data as possible. Monitoring and logging data that you do not need uses up disk space and processing power, and generates extra network traffic. There are several areas where you can implement your strategy:

Database monitoring

The global SQL monitor captures SQL information and puts it into a queue for the S-TAP. You can use the filtering capabilities of the monitor to control which types of users and objects are queued. By default, these types of entries are not forwarded from the S-TAP to the Guardium® system:

| SQL Abbreviation | Meaning |
|------------------|--|
| AD | ALLOCATE DESCRIPTOR |
| CL | CLOSE |
| DA | DEALLOCATE DESCRIPTOR |
| DE | DESCRIBE |
| EX | EXECUTE (the SQL statement executed is audited) |
| FE | FETCH |
| FL | FREE LOCATOR |
| GD | GET DIAGNOSTICS |
| GS | GET DESCRIPTOR |
| HL | HOLD LOCATOR |
| PR | PREPARE (except authorization errors are captured) |
| RE | RELEASE |
| RG | RESIGNAL |
| SC | SET CONNECTION |
| SD | SET DESCRIPTOR |
| SG | SIGNAL |

Audit journal

You can configure the system audit journal to capture only those entries that concern objects of interest or users of interest. By default, entries of these types are sent from the S-TAP to the Guardium system:

| SQL Abbreviation | Meaning |
|------------------|------------------------------|
| ZR | Read object |
| ZC | Change object |
| CA | Authority change |
| AD | Auditing change |
| AF | Authority failure |
| CO | Create object |
| DO | Delete object |
| SV | System Value change |
| GR | General purpose audit record |
| OM | Object moved or renamed |
| PG | Primary group change |
| PW | Invalid password or user ID |
| OW | Change owner |
| OR | Object restored |
| RA | Restore authority change |
| RO | Restore owner change |
| RZ | Restore primary group change |

Only those entries that relate to database objects are forwarded:

- *FILE (a table, view, index, logical file, alias, or device file)
- *SQLUDT (an SQL user-defined type)
- *SQLPKG (an SQL package)
- *PGM (a procedure, function, or program)
- *SRVPGM (a procedure, function, global variable, or service program)
- *DTAARA (an SQL sequence)

On the Guardium system

You can define policies that control which information that is received from the S-TAP is ignored, and what actions to take based on other items.

Ignoring data after it has been sent over the network is inefficient. Wherever possible, filter out information that you do not need before it is queued for the S-TAP.

Installing the S-TAP for IBM i

The S-TAP software is a shell script that you must run from IBM i, within the Portable App Solutions Environment (PASE) environment. Take the following steps to upload the S-TAP software to the IBM i Integrated File System (IFS) and then install it.

Before you begin

- Review the minimum requirements from the following location: [Guardium and Db2 for i - technical resources](#)
- Review the Db2 for IBM i PTF Group Schedule for your version of IBM i: [Db2 for i - Technology Updates](#).
- Make sure that you have the following special authorities: *ALLOBJ, *JOBCTL, and *SECADM.
- Verify that license program 5722SS1-33 Portable App Solutions Environment (PASE) is installed on your IBM i system.

- If you use FTP to upload S-TAP software to IFS, ensure that you have access to the 5250 emulator software to connect to the IBM i system remotely. To use the IBM i Access Client Solutions (ACS) tool, download ACS from the following location: [IBM i Access Client Solutions](#).
- Download the S-TAP for the IBM i platform.
- Identify the IP address of the Guardium® system to which this S-TAP connects.
- Ensure that the following ports are open between the Guardium system and IBM i:
 - Port 446: The default port for data source connectivity via JDBC.
 - Port 16016: the port for sending encrypted traffic to the Guardium collector.

Note: In general, connections to the following IBM i ports are required:

- 449
- 446/448(TLS/SSL)
- 8471/9471(TLS/SSL)
- 8476/9476(TLS/SSL)

However, depending on the version of the IBM i server and the version of the jt400.jar JDBC driver that Guardium uses, the required ports might vary. See the [IBM i Documentation](#) to check the IBM i well-known ports. For more information about port requirements for IBM i, see [TCP/IP Ports Required for IBM i Access and Related Functions](#).

- Use the IBM i Verify TCP/IP Connection (PING) command to verify that IBM i can establish a TCP/IP connection to the IP of the Guardium system that the S-TAP must communicate with.

Procedure

1. Upload the S-TAP software to the IBM i Integrated File System (IFS) by using FTP or the graphical IBM i Access Client Solutions (ACS) tool.

To upload via FTP, use the following steps:

- Use the 5250 emulator software to connect to IBM i remotely and enter the following command to open the PASE shell: **call qp2term**.
- In the PASE shell environment on the IBM i, create a temporary directory to store the S-TAP installation script. Example: /tmp/username.
- Use the start TCP/IP File Transfer (FTP) command and move the S-TAP installation shell script to that temporary directory.

To upload by using ACS, use the following steps:

- Within the ACS tool, use the IFS to create a temporary directory and navigate to it.
- Use the GUI to select and upload the S-TAP software.

2. In the temporary directory, run the following command:

```
<S-TAP_shell_script.sh> --sqlguardip <guardium_host_IP> -u |  
-overwrite-existing [--tls force | none]
```

Where:

- --sqlguardip: a mandatory parameter that indicates the IP address of the Guardium system with which the S-TAP communicates.
- If an IBM i S-TAP installation exists, you must enter one of the following parameters:
 - -u: an optional parameter to keep the existing configuration parameters and update the S-TAP configuration with the parameters that were entered in the command.
 - -overwrite-existing: an optional parameter to overwrite the existing installation and create a new guard_tap.ini file with default parameters.
- --tls force: an optional parameter to use TLS encryption. If a secure protocol cannot be obtained when you connect, the S-TAP can fall back to using a nonsecure protocol.
- --tls none: an optional parameter to indicate that the connection is not encrypted. This parameter is selected by default if TLS is not specified.

The program installs in the following location: /usr/local/guardium.

3. Optional: When you install the S-TAP, it not only installs the necessary components and configurations, but the S-TAP also starts with the factory default configuration. Therefore, the S-TAP immediately starts capturing all database activity for all users and processes. You can stop the S-TAP immediately after installation, establish filtering rules, and then restart the S-TAP.

To stop the S-TAP, use the IBM i Run SQL command. For example,

```
RUNSQL SQL('CALL SYSPROC/SYSAUDIT_END()') COMMIT(*NONE)
```

Tip: You must establish a filtering rule that matches your database activity monitoring strategy and requirements. As an example, if you use only the Guardium policy to establish filtering, the S-TAP on IBM i might transfer and store more activity details than needed on the Guardium collector.

4. On the Guardium system's GUI, go to Manage > System View > S-TAP Status Monitor and confirm that the S-TAP status is green. A green status indicates that the S-TAP is communicating with the collector. If the S-TAP monitor is not showing green, review the details within the following IFS stream files:

- /usr/local/guardium/install_out.txt
- /usr/local/guardium/guard_itap.stderr.1.txt

Tip: You can ignore the Inspection Engine status column. Inspection engines are not used for Db2 for i S-TAP.

Uninstalling the S-TAP

Procedure

To stop and uninstall the S-TAP, run the following commands:

```
RUNSQL SQL('call SYSPROC/SYSAUDIT_End') COMMIT(*NONE)  
CALL QR2TERM  
cd /usr/local/guardium/  
uninstall  
F3  
RMVDIR DIR('/usr/local/guardium') SUBTREE(*ALL)
```

Upgrading the S-TAP from 10.x to 11.x for IBM i

About this task

Procedure

1. Use FTP to save the 11.3 itap onto iSeries using binary mode. For example,

```
ftp <server name>
username/password
cd /usr/diver
binary
put itap-11.3.sh
```

2. Stop the v10.0.0 itap audit server in the 5250 terminal with:

```
RUNSQL SQL('CALL SYSPROC/SYSAUDIT_END( )') COMMIT(*NONE)
```

3. Upgrade the i S-TAP

```
CALL QP2TERM
$ 
> cd /usr/diver
$ 
> itap-11.3.sh --sqlguardip guardclient.rch.stglabs.ibm.com -u
Verifying archive integrity... All good.
Uncompressing guard-itap.....
Checking whether Audit Server has been stopped. (This call may take a minute.
Please wait.)
Uninstalling.
Creating /usr/local/guardium directory.
Using sqlguard_ip=guardclient.rch.stglabs.ibm.com
Starting Audit Server.
```

\$
The upgrade is successful.

4. Verify the upgrade.

- a. In the 5250 terminal, verify that this string appears: /istap log_file=

```
> ps -ef
UID PID PPID C STIME TTY TIME CMD
qsecocr 10 8 0 Dec 03 - 0:23 /QOpenSys/QIBM/ProdData/JavaVM
qsys 58 1 0 Dec 03 - 14:07 /QIBM/ProdData/OS/SLP/bin/lslp
ruiyu 754 753 0 Feb 18 - 0:00 /QOpenSys/usr/bin/-sh -i
qlwsvr 857 1 0 Feb 26 - 4:39 /QOpenSys/QIBM/ProdData/JavaVM
qlwsvr 858 1 0 Feb 26 - 10:21 /QOpenSys/QIBM/ProdData/JavaVM
qlwsvr 859 1 0 Feb 26 - 0:40 /QOpenSys/QIBM/ProdData/JavaVM
qlwsvr 860 1 0 Feb 26 - 0:33 /QOpenSys/QIBM/ProdData/JavaVM
4294770734 861 1 0 Feb 26 - 0:44 /QOpenSys/QIBM/ProdData/JavaVM
richoj 1102 988 0 17:56:33 - 0:00 /QOpenSys/usr/bin/-sh -i
richoj 1243 1236 0 17:57:53 - 0:00 ./istap log_file=
richoj 1244 1102 0 17:58:35 - 0:00 ps -ef
$
```

- b. In the 5250 terminal, verify that you see the 11.3x.0.swidtag

```
> cd /usr/local/guardium/
> ls
LICENSE.TXT istap sqsh
guard_itap.stderr.1.txt istap_console.socket sqsh_write_file
guard_tap.ini just_send swidtag
install_out.txt libprotobuf.a uninstall
$ 
> cd swidtag
$ 
> ls
ibm.com_IBM_Security_Guardium_Data_Protection-11.3.0.swidtag
$
```

- c. In the Guardium S-TAP Control page, verify that the 11.x itap connections are green for iSeries 7.4 (SQ740) and iSeries 7.3 (UT28P55).

Defining the S-TAP for IBM i

After you install the S-TAP, ensure that it can communicate with the Guardium® system.

Before you begin

You must know the log-in credentials for the IBM i system.

About this task

The high-level steps to configure the S-TAP are:

1. Define Db2 for i as a recognized data source to IBM® Guardium and test the connection.
2. Populate the Guardium system with information from the configuration file on IBM i that was created when you installed the Db2 for i S-TAP, using the Custom Table Builder process.
3. Create a Db2 for i configuration report. It is from this report interface that you can invoke the Guardium APIs that enable you to start and stop the monitoring process, get status information, and update configuration parameters, including filtering values.

Procedure

1. Click Setup > Tools and Views > Datasource Definitions to open the Datasource Builder.
2. In the Datasources Definitions page, click . The Create Datasource dialog opens.
3. Fill in values:
 - Application Type: Custom Domain.
 - Database Type: Db2 FOR i.
 - all other fields: as relevant for your system.
4. Click Save.
5. Click Test Connection to ensure that the configuration succeeded.
6. Click Comply > Custom Reporting > Custom Table Builder.
7. Select Db2 for i S-TAP Configuration, and then click Upload Data.
8. Click Add Datasource.
The Select datasource window displays a list of Db2 for i S-TAPs
9. Select your Db2 for i data source from the list and click Save.
10. On the Import Data page, ensure the Db2 for i data source appears. Click Apply and then click Run Once Now.
A message appears that the operation ended successfully with one row inserted.
11. Click Comply > Custom Reporting > Custom Query-Report Builder.
12. From the Queries-Reports list, click Db2 for i S-TAP configuration, then click Open original.
13. Click Add to My Custom Reports.
14. Click Reports > My Custom Reports, and open the Db2 for i S-TAP configuration report, which now displays the IBM i report row. Right-click a row in the report and select Invoke. A list of APIs appears.
15. Select update_istap_config.
The parameters for that API are displayed. You can change any values.
16. Change the value of the start_monitor parameter to 1.
17. Click Invoke Now.

Results

Using the data that you have entered, the [update_istap_config](#) API performs these tasks:

- Creates the message queue that is used to send entries from the S-TAP to the Guardium system and starts a global database monitor using a view with an INSTEAD OF trigger, which sends the entries to the message queue.
- Starts PASE and the S-TAP.
- Receives journal entries from QAUDJRN and adds them to the message queue.

Related reference

- [S-TAP for IBM i APIs](#)

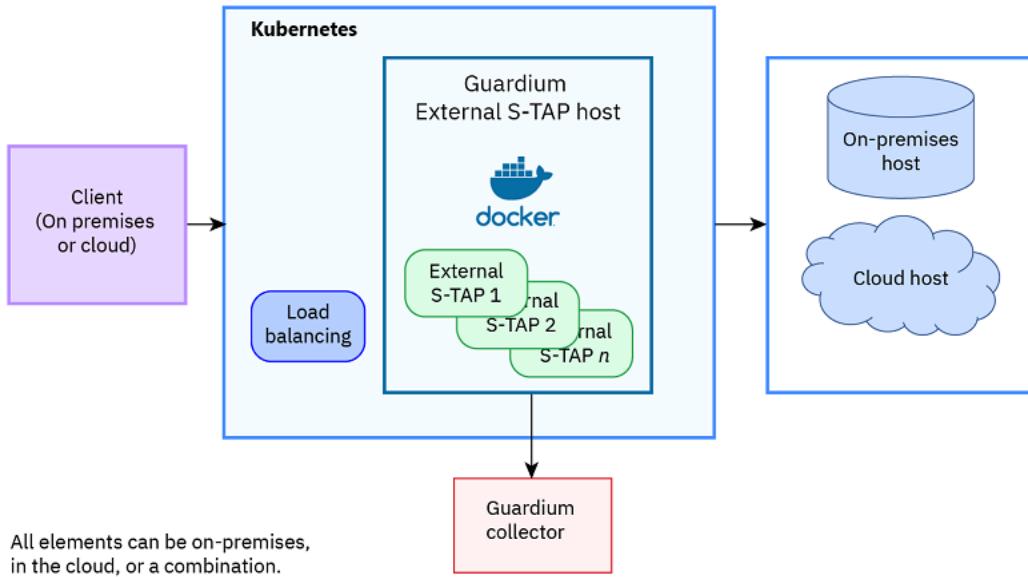
External S-TAP

IBM® Guardium® External S-TAP is a component of Guardium that can intercept traffic for cloud and on-premises database services without installing an agent on the database server. You can either deploy an External S-TAP with Kubernetes on the OpenShift® platform or manually (without Kubernetes).

External S-TAP intercepts traffic between clients and the database server, and forwards a copy of the traffic to a Guardium collector for analysis and policy application. After your External S-TAPs are installed and running, your External S-TAPs support many S-TAP policies, including redaction, S-GATE, and S-TAP Terminate. For more information about applying policy rules, see [Policy rule actions](#).

As shown in [Figure 1](#), you can use External S-TAP with Kubernetes with either cloud and on-premises databases. If your site does not use Kubernetes, you can deploy External S-TAPs manually, as shown in [Figure 2](#). For more information, see [External S-TAP requirements](#).

Figure 1. External S-TAP overview with Kubernetes

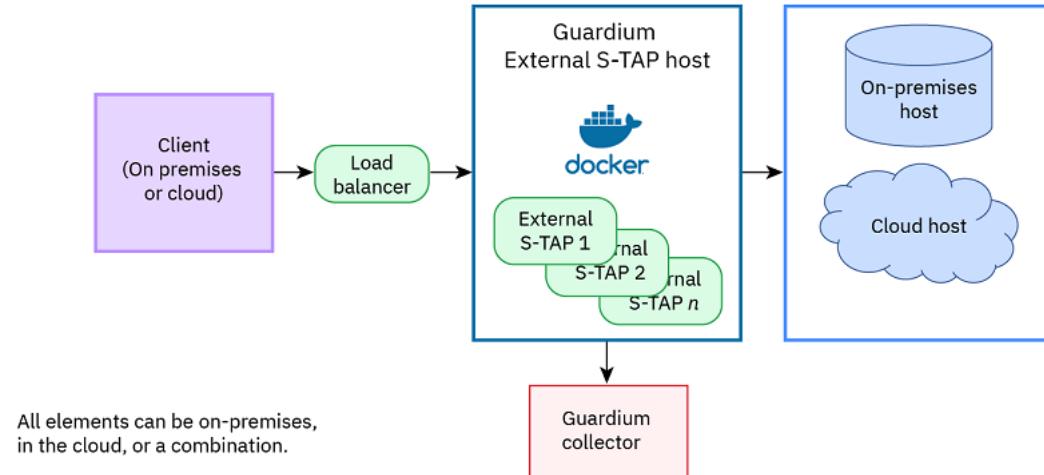


As shown in [Figure 1](#), all elements of a Guardium system that use External S-TAP can be either on premises or in the cloud. If your site uses Kubernetes, then Kubernetes takes care of many housekeeping issues such as balancing the software load and managing Docker containers. In the Kubernetes deployment configuration, specify the Docker image to use for the pods. To verify the collector certificates, as described in [Verify collector certificates \(optional\)](#), specify your private repository along with the derived Docker image name and tag. If your site does not use Kubernetes, you need to download the External S-TAP Docker container and deploy a load-balancing solution through a hardware appliance or software. For more information, see [Load balancer scripts](#).

As an alternative to deploying the External S-TAP with Kubernetes, you can use Helm charts to simplify the deployment. For more information, see [Deploying External S-TAP with Helm](#).

For information about installing External S-TAP without Kubernetes, see [Deploying External S-TAP manually](#).

Figure 2. External S-TAP overview, manual installation



As shown in [Figure 2](#), all elements of a Guardium system that use External S-TAP can be either on premises or in the cloud. External S-TAP is highly configurable. During deployment, you can configure most options, as discussed in [External S-TAP deployment scripts](#). Balancing the load can either be done through a hardware appliance or software. For more information about deploying a load-balancing solution, see [Load balancer scripts](#).

The Guardium External S-TAP Docker container

Docker containers provide a way to package software solutions so that you can easily download and manage them. Depending on your site configuration, a Guardium External S-TAP Docker container can either be downloaded directly from the IBM Cloud Container Registry (icr.io) or for computers without internet access, from a private image repository.

A Docker container runs an image, which is a packaged software solution (in this case, an External S-TAP) that can be installed on your host database. You can install multiple containers on the machine that serves as the External S-TAP host.

You can choose to derive the Docker container image by using a Dockerfile. By deriving the image, you can specify a single Guardium collector certificate (or set of related certificates) that you can use to deploy the External S-TAP. For more information, see [Verify collector certificates \(optional\)](#).

Before you deploy an External S-TAP

Assuming that your site is already using Guardium, the following steps are needed for each database where you want to run an External S-TAP container.

- If your site manages encrypted traffic (that is, is SSL-enabled), you need to work with a certificate authority (CA) to prepare the Guardium collector with the appropriate security certificates. This step can take some time, since you need to work with an outside company (the CA). For more information, see [SSL certificates for External S-TAP](#). If your environment is not SSL-enabled, you can skip this step.
- Make sure that a Linux® environment is available. Docker must be installed and running under Linux. For more information, see <https://www.docker.com/> and [Download the Docker container](#).
- Prepare to deploy an External S-TAP:
 - If your site uses Kubernetes, you can deploy an External S-TAP via the user interface. To deploy with Kubernetes from the Guardium UI, use one of the following services:
 - Amazon Elastic Container Service for Kubernetes (Amazon EKS)
 - Microsoft Azure Kubernetes Service (AKS)
 For more information, see [Deploying External S-TAP from the Guardium UI](#).
 - If your site does not use Kubernetes, you need to run scripts to deploy both a load balancer and the External S-TAP. Skip the section on deploying the External S-TAP with Kubernetes and go directly to [Deploying External S-TAP manually](#).

After you deploy the External S-TAP, it runs automatically. You can manage the External S-TAP from the Guardium UI. For more information, see [The External S-TAP user interface](#).

- [External S-TAP requirements](#)**

To use External S-TAP with your IBM Guardium system, your site must meet the following requirements.

- [SSL certificates for External S-TAP](#)**

To help protect SSL-enabled systems, the Guardium External S-TAP requires that you acquire a Secure Socket Layer (SSL) digital certificate for a TLS-encrypted database. If your database environment is not SSL-enabled, you can skip this step.

- [Deploying External S-TAP with an operator](#)**

Use Kubernetes with a computer assisted software engineering (CASE) operator to deploy your External S-TAPs. You can deploy External S-TAP as a stand-alone service, similar to installing and running the External S-TAP from Cloud Pak for Data v 4.0.

- [Deploying External S-TAP with Helm](#)**

Use Kubernetes with Helm to automate your External S-TAPs deployment.

- [Deploying External S-TAP from the Guardium UI](#)**

If your site uses Kubernetes, you can deploy an External S-TAP directly from Guardium.

- [Deploying External S-TAP manually](#)**

Deploy an External S-TAP with Docker and the External S-TAP scripts.

- [The External S-TAP user interface](#)**

Use the External S-TAP instances page to create, monitor, start, stop, and configure Guardium External S-TAPs.

- [Best practices for using External S-TAPs with on-premises databases](#)**

To use External S-TAPs with on-premises databases, you need to take a few steps to prepare both your database and the External S-TAP. Examples are shown using PostgreSQL.

- [Configuring AWS HA for External S-TAPs](#)**

Include External S-TAPs in your existing Amazon AWS high availability (HA), or failover, configuration.

- [Configuring Google BigQuery for External S-TAPs](#)**

Include External S-TAPs in your Google BigQuery configuration for Guardium.

- [Troubleshooting External S-TAP issues](#)**

Check for solutions if something goes wrong with your External S-TAPs.

External S-TAP requirements

To use External S-TAP with your IBM® Guardium® system, your site must meet the following requirements.

For more information about supported platforms for External S-TAP, see [IBM Guardium System Requirements and Supported Platforms](#).

Use Kubernetes on the Red Hat OpenShift platform to manage containers for External S-TAP. However, you can manually manage Docker containers by using the script that is described in [External S-TAP deployment scripts](#). A load-balancing solution is also required, which can be provided as part of your cloud service provider's Kubernetes services. If your site does not use Kubernetes, Guardium provides a sample script to help you configure your load-balancing solution. For more information, see [Load balancer scripts](#).

Important: The CN that you specify to create the certificate signing request (CSR) for the External S-TAP must match the DNS name to which the clients are connecting. For External S-TAP, the CN is the DNS name for the load balancer. If the client database requires that the DN (Designated Name) match the DNS entry, then all the properties in the CSR (such as CN= or OU=) must also match the DNS entry.

For administrators, you can redirect the clients to the External S-TAP by adjusting the DNS resolution. If you change the DNS resolution, be sure to use the DNS name that is visible to the client (that is, the name of the database server).

The External S-TAP can listen to only one port per container.

External S-TAP supports both unencrypted (plain text) and SSL/TLS-encrypted session flows. Other types of encrypted workflows (such as TDGSS and Oracle Native Encryption) are not supported.

If the External S-TAP container host is an on prem or virtual machine, the host must meet the following requirements:

- An x86_64 processor.
- Minimum RAM memory 500 MB and 2 GB storage.
- Linux® kernel version 3.10 or higher (latest version is recommended).
- Iptables 1.4 or higher.
- Docker Desktop.
- Minimum 2 virtual CPUs.
- Ability to use UNIX domain sockets.

Important: For on-premises installations, enable pubkey authentication for the user who starts the containers on the host systems. The deployment script calls `ssh` for the host systems multiple times; pubkey authentication simplifies the process.

You can include persistent volumes for storage to keep External S-TAP information after the Docker or Kubernetes container has exited. To use a persistent volume,

- For Kubernetes, configure the storage to appear inside any containers at `/persistent`. For more information, see [Deploy External S-TAP window](#).

- For container_mgmt.sh, use the **--persistent** flag to specify the name of the Docker volume to use. For more information, see **--persistent** in [External S-TAP deployment scripts](#).

All installations, either on prem or in the cloud, must meet the following requirements:

- For Docker, make sure that the installing user has the necessary privileges to create a container across systems.
- Make sure that network access is available to the IBM Cloud Container Registry (icr.io) where IBM releases the External S-TAP images.
- Database clients must be able to use TCP to connect to the External S-TAP host and the External S-TAP host must be able to connect to the database server.
- Locate all External S-TAP hosts in the network topology in such a way that they can be placed between the client and database host. Ideally, the latency between the client, the External S-TAP host, and the database service is as brief as possible.
- Be sure that access to the External S-TAP host is secured.
- Docker uses the kernel core pattern of the host to determine where to place core files. On some systems, the default path is not appropriate from the container's perspective. To make sure that core files are stored correctly, use the following pattern:

```
'/tmp/core.%t.%e.%p'
```

For example, on the External S-TAP host where a container runs, enter the following command to set the core pattern:

```
echo '/tmp/core.%t.%e.%p' | sudo tee /proc/sys/kernel/core_pattern'
```

Microsoft Azure users: The Azure SQL database connection policy is set to Redirect by default. You need to set the policy to Proxy. For more information, see [Azure SQL Connectivity Architecture](#) in the Microsoft Azure documentation.

In addition, to connect to the database, you need to update the `/etc/hosts` file for your system to add the following entry:

<External-IP> <your DB host>

- For Windows, add this entry to `\windows\system32\drivers\etc\hosts`.
- For Linux or UNIX, add this entry to `/etc/hosts`.

AWS Network Load Balancer users: AWS Network Load Balancer does not support listening on multiple public IP addresses. You can't listen twice on the same port for the same IP. Therefore, if your site is using multiple IP addresses, you must use a separate load balancer for each IP address.

Active directory database: For databases with active directory authentication, update the `/etc/hosts` file for your client system to add the following entry:

<External-IP> <your DB host>

- For Windows, add the entry to `\windows\system32\drivers\etc\hosts`.
- For Linux or UNIX, add the entry to `/etc/hosts`.

Note: When you deploy External S-TAP with the AWS load balancer, AWS load balancer can have multiple IP addresses. Make sure that you use the **<External-IP>** that can connect to the load balancer.

SSL certificates for External S-TAP

To help protect SSL-enabled systems, the Guardium® External S-TAP requires that you acquire a Secure Socket Layer (SSL) digital certificate for a TLS-encrypted database. If your database environment is not SSL-enabled, you can skip this step.

With External S-TAP there are two ways in which you can configure SSL certificates for your Guardium system:

- Recommended: [Configure on-demand certificate generation](#) by storing an intermediate certificate on the Guardium central manager or collector. Guardium can use that certificate to automatically generate certificates for every External S-TAP container.
- [Manually create a certificate signing request](#) and then store the certificates on any Guardium collectors that use External S-TAP.

Note: Guardium does not provide CA services.

After you configure the certificates for the central manager, you can use the [pull_external_stap_keystore](#) GuardAPI to copy the keystore from the central manager to one or more managed units.

- [Configure on-demand certificate generation](#)**

Configure Guardium External S-TAPs to automatically generate certificate signing requests (CSRs) that are signed by an intermediate certificate.

- [Manually create a certificate signing request](#)**

Create a certificate signing request (CSR) for each Guardium External S-TAP you want to manually deploy for an SSL-enabled database. Within the generated CSR, this procedure also creates the token (the shared secret) that you need to install the External S-TAP.

- [Verify collector certificates \(optional\)](#)**

You can help ensure that your External S-TAP connects only to an authorized collector by verifying the collector's certificate before connecting to the External S-TAP.

- [Verifying client and server certificates](#)**

To provide an extra level of security, you can store server or client certificates in a custom keystore, explicitly include or exclude known certificates in the keystore, or both.

- [Importing a custom certificate](#)**

To integrate External S-TAP for a server with server verification or mutual authentication if your database uses a custom certificate (that is, a trusted root certificate signed by a certificate authority [CA]), then External S-TAP must import the custom certificate. To do so, you need to build a container image, and then manually import the custom certificate.

- [Configuring mutual authentication](#)**

If your database settings are configured for mutual authentication, you can configure the External S-TAP, to verify the certificate that is set from both the data store server and client.

- [Configuring certificate mirroring](#)**

Certificate mirroring allows an External S-TAP to automatically generate copies of client and server key pairs from an existing signing key pair. Use certificate mirroring to provide mutual authentication for sites with more than one client certificate.

- [Preparing SSL certificates for client applications](#)**

To use client applications with External S-TAP, you might need to update the database client by specifying a new database endpoint and port from External S-TAP.

Configure on-demand certificate generation

Configure Guardium® External S-TAPs to automatically generate certificate signing requests (CSRs) that are signed by an intermediate certificate.

About this task

Store an intermediate certificate on a Guardium collector to allow External S-TAP instances to sign a certificate request from an External S-TAP that uses your common name (CN) to create an on-demand certificate for encrypted traffic. In this case, the CSR and the signed certificate carry the public key.

Note: If your database configuration requires a CN match, specify the name of either the server or the load balancer as the CN.

Procedure

1. Obtain an intermediate signing key and certificate pair from your certificate authority.

Note that Guardium does not provide certificate authority.

2. Use the following CLI command to store the signing key and signing certificate on the Guardium system as an intermediate certificate:

```
store certificate_external_stap_signing
```

At the prompts, enter the requested information, exactly as it shows in your certificate. Only the common name (CN=) is required.

3. The command generates a token that is required to deploy the External S-TAP. The token is the certificate secret, which you provide in either the Guardium GUI or the deployment script. Record the token because you will need it to deploy External S-TAPs in the future.

Note: You can view the token by calling **show certificate external_stap_signing**. To create a new token, delete the certificate by using **delete certificate external_stap_signing** and then store it again.

- In the GUI, enter the details in the Container tab of the Deploy External S-TAP window.
- In the deployment script, enter the details in the --proxy-secret and --proxy-csr-name parameters (along with any other parameters that you include).

What to do next

After the intermediate certificate is stored on the collector, it can automatically create a certificate for each new External S-TAP container.

Related concepts

- [Certificate CLI commands](#)
- [External S-TAP deployment scripts](#)

Related reference

- [Deploy External S-TAP window](#)

Manually create a certificate signing request

Create a certificate signing request (CSR) for each Guardium® External S-TAP you want to manually deploy for an SSL-enabled database. Within the generated CSR, this procedure also creates the token (the shared secret) that you need to install the External S-TAP.

About this task

Take the following steps to create a certificate request and token and then store the certificate in the External S-TAP keystore.

Procedure

1. Enter the following CLI command:

```
create csr external_stap
```

2. When prompted, enter an alias for the certificate, which can be the hostname, or any meaningful name:

```
host.example.com
```

3. At the prompts, enter the following information, exactly as it displays in your certificate:

- The common name (CN=) for this certificate, which must be the fully qualified domain name of the load balancer. If your site uses Kubernetes, you can find the domain name of the load balancer in the Kubernetes console as External endpoint. For example,

```
example.yourdomain.com
```

- The organizational unit (OU=), for example **external_stap**.
- The name of your organization (O=), for example **IBM**.
- The name of your city or locality (L=), for example **Boston**.
- The code for your state or province (ST=), for example **Massachusetts**.
- The two-letter country code for the unit (C=), for example **US**.
- The encryption algorithm to use (1 = DSA, 2 = RSA [default]), for example, **2**.

4. After you enter the requested information and press **Enter**, the certificate request process begins. When prompted, enter the following information:

- The keysize to use (1 = 1024, 2 = 2048 [default]), for example **2**.
 - Up to 99 SANs (Subjective Alternative Names) in fully qualified domain name format. To continue without entering a SAN, press Enter.
5. The system generates and displays the CSR.
6. Copy and paste the entire certificate signing request (CSR) into a file (in an editor such as Notepad).
Note: The CSR output includes an alias in the format **CN proxy_keycert token**. You need the alias to store the certificate.
7. Then, copy and paste the certificate request into a file to send to the CA. The certificate request is all of the information between (and including) the BEGIN and END statements. That is, be sure to include all of the text, starting with the following line:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
```

And ending with the following line:

```
-----END NEW CERTIFICATE REQUEST-----
```

What to do next

After the certificate is returned from the CA, you can store it on the Guardium collector or a Guardium central manager (CM), as follows:

1. Store the root and intermediate certificates from the CA with the following command:

```
store certificate keystore_external_stap
```

2. Store the signed certificate on the collector or central manager with the following command:

```
store certificate external_stap
```

Note: If the certificate is not already in PEM format, use OpenSSL or another third-party tool to convert it.

For example, to convert from PKCS7 format to PEM, use the following OpenSSL command:

```
openssl pkcs7 -print_certs -in certificate.p7b -out certificate.pem
```

3. When prompted, enter the alias for the signed certificate, which was included in the CSR output file.

Note: If you do not remember the alias, use the **show certificate external_stap** command to display the certificate information. For more information, see [Certificate CLI Commands](#).

4. You can now deploy the External S-TAP:
 - If your site uses Kubernetes, see [Deploying External S-TAP from the Guardium UI](#).
 - If your site does not use Kubernetes, see [Deploying External S-TAP manually](#).

Related concepts

- [Certificate CLI Commands](#)

Verify collector certificates (optional)

You can help ensure that your External S-TAP connects only to an authorized collector by verifying the collector's certificate before connecting to the External S-TAP.

About this task

To verify the collector's certificate, provide the External S-TAP CA certificate and the CN for the collector's certificate. If your site uses Kubernetes, specify your private repository along with the derived Docker image name and tag as the image to use for the pods in the deployment configuration.

Procedure

1. Create and store a certificate signed request (CSR) on the collector with the **create csr sniffer** CLI command as described in [Configuring Guardium-S-TAP communication using an SSL certificate](#).
2. Instead of downloading a Docker image from the IBM Cloud Container Registry (icr.io), derive the Docker container image from the icr.io to add the CA certificate to the /etc/guardium/guardium_ca.crt file. For example, to derive the latest version of the External S-TAP Docker container, add the following commands to your Dockerfile:

```
FROM icr.io/guardium-insights/guardium_external_s-tap:latest
COPY ./guardium_ca.crt /etc/guardium/guardium_ca.crt
```

Note: The entire COPY path is required: **/etc/guardium/guardium_ca.crt**.

3. From the derived container, run the **docker build** command create a new docker image. For example:

```
docker build -t localhost/<my_image_name>:latest .
```

4. When you deploy a new External S-TAP, provide the derived image and configure the External S-TAP to expect the CN of the collector's certificate. You can deploy the External S-TAP in multiple ways:

- From the user interface in the Advanced tab under the Deploy External S-TAP tab:
 - Select Verify certificate
 - In Collector CN, provide the collector's certificate CN. You can use a regular expression to verify multiple certificates.

For more information, see [Deploy External S-TAP window](#)

- From the **container_mgmt.sh** script in non-interactive mode, provide the collector's certificate CN in the --sqlguard-cert-cn parameter. For more information, see [External S-TAP deployment scripts](#).

- From the **container_mgmt.sh** script in interactive mode, enter the collector's certificate CN in response to the following question:

Enter the CN to match when verifying the Guardium Collector's Certificate

What to do next

After you deploy the External S-TAP, the External S-TAP starts. You can make sure that it is running from the External S-TAP instances pane.

Verifying client and server certificates

To provide an extra level of security, you can store server or client certificates in a custom keystore, explicitly include or exclude known certificates in the keystore, or both.

Configure client and server certificates for the External S-TAP

In this scenario, you want to use the External S-TAP custom keystore verify that the External S-TAP communicates only with trusted clients and servers.

1. Configure the External S-TAP to trust your data store server certificate, you need the one of the following certificates:

- The signed certificate from your data store server, along with the token that was provided to create the certificate signing request (CSR). In this case, use the following CLI command to store the signed certificate in a custom keystore on the External S-TAP:

```
store certificate custom_keystore_external_stap
```

When prompted, supply the following information:

- The alias for the signed certificate, which was included in the CSR output file.
- The token that was provided to create the CSR.
- A self-signed certificate from your data store server. In this case, you can store the certificate directly into the allowlist, as described in [Certificate allowlists and blocklists](#).

2. Configure the data store client to trust the External S-TAP certificate, by taking one or both of the following steps:

- If the client can accept a trusted certificate, then store the signed External S-TAP certificate on the client data store.
- If the client can trust a certificate based on allowlist, you can also store the External S-TAP directly.

Note: If your site is using PostgreSQL for both the client and server data stores, you can additionally configure the server to trust the External S-TAP certificate to create a mutual authentication scenario. For more information, see [Configuring mutual authentication](#).

Certificate allowlists and blocklists

In addition to using certificates to verify communication with the External S-TAP, you can use allowlists and blocklists to explicitly define which certificates your site can, or cannot, trust. The lists are stored in the custom keystore.

You can add one or more certificates to an allowlist to explicitly trust the certificates on a client or server machine. In addition, you can explicitly exclude, by using a blocklist, certificates that you know can no longer be trusted.

Note: Certificates can be added only one at a time.

Use the following CLI command to add a certificate to a trusted list (an allowlist):

```
store certificate allowlist_external_stap
```

Use the following CLI command to explicitly exclude a certificate (a blocklist):

```
store certificate blocklist_external_stap
```

When you add a certificate to either an allowlist or a blocklist, you are prompted for the following information:

- The alias for the signed certificate, which was included in the CSR output file.
- The token that was provided to create the CSR for the External S-TAP certificate.

Note: For an added level of security, you can optionally use the certificate that you created to verify the collector's certificate. For more information, see [Verify collector certificates \(optional\)](#).

Other certificate CLI commands

To delete one or more certificates from the keystore, use the following CLI command:

```
delete certificate external_stap
```

A numbered list of all of the certificates in the keystore displays. Select the certificates to delete, by their number. To delete multiple certificates, separate each number with a comma.

To show details about the certificates in the keystore, use the following CLI command:

```
show certificate external_stap
```

For each certificate, useful information such as alias name, entry type, owner, and valid dates displays.

For more information about certificate-related CLI commands, see [Certificate CLI commands](#).

Note: To determine the actions to take when Guardium encounters an invalid certificate, set the actions in either the External S-TAP tab or the deployment script. For more information, see [External S-TAP tab](#) or the --invalid-cert-disconnect and --invalid-cert-notify parameters in [Table 3](#).

Importing a custom certificate

To integrate External S-TAP for a server with server verification or mutual authentication if your database uses a custom certificate (that is, a trusted root certificate signed by a certificate authority [CA]), then External S-TAP must import the custom certificate. To do so, you need to build a container image, and then manually import the

custom certificate.

Procedure

1. Download the External S-TAP image from the IBM Cloud Container Registry (icr.io). Derive the docker container image from the *icr.io* to add the ca.cert custom CA certificate to the /etc/ssl/certs/ca-bundle.trust.crt file.

For example, to derive the latest version of the External S-TAP docker container, add the following commands to your Dockerfile:

```
FROM icr.io/guardium-insights/guardium_external_s-tap:latest
COPY ./ca.crt /etc/ssl/certs/ca-bundle.trust.crt
```

2. From the derived container, run the **docker build** command create a new docker image, for example:

```
docker build -t localhost/guardium_external_s-tap:v12.0 . -f Dockerfile
```

3. When you deploy a new External S-TAP, provide the derived image and configure the External S-TAP to verify the database server certificate. You can use one of the following methods:

- From the container_mgmt.sh script, edit the following parameters:

```
--invalid-cert-disconnect
--invalid-cert-notify
```

- With a helm chart, edit the following information:

```
# Verify certificates and disconnect if they are invalid
# Optional, default is 0 (no)
disconnect_on_invalid_certificate: true

# Verify certificates and send a message to the STAP event log
# if they are invalid
# Optional, default is 0 (no)
notify_on_invalid_certificate: true
```

- Configure the On invalid certificate parameter in the Guardium UI (from the External S-TAP tab in the Edit External S-TAP group page).

Configuring mutual authentication

If your database settings are configured for mutual authentication, you can configure the External S-TAP, to verify the certificate that is set from both the data store server and client.

About this task

For the External S-TAP, Guardium supports mutual authentication through an External S-TAP custom keystore. In this scenario:

1. The data store client successfully verifies the certificate in the External S-TAP custom keystore.
2. The External S-TAP verifies the data store server certificate.
3. If mutual authentication is enabled on both the client and the server, the client sends the client certificate to the External S-TAP. The External S-TAP parses that message and verifies the certificate on behalf of the server.
4. If the client certificate is trusted, External S-TAP sends the External S-TAP certificate to the PostgreSQL server so that the PostgreSQL server can verify the certificate from the External S-TAPs.

To provide mutual authentication with multiple client certificates, you need to use certificate mirroring. For more information, see [Configuring certificate mirroring](#).

Procedure

1. To configure the External S-TAP to trust your data store client certificate, you need the CA-signed certificate (or certificates) from the client data store.

Note: Make sure that all certificates (for the External S-TAP, the client, and the server) are signed by the same certificate authority.

Use the following CLI command to store the signed client certificate into the External S-TAP custom keystore:

```
store certificate custom_keystore_external_stap
```

When prompted, supply the following information:

- The alias for the signed certificate, which was included in the CSR output file.
- The token that was provided to create the CSR for the External S-TAP certificate.

2. To verify a client certificate on a PostgreSQL server, import the External S-TAP certificate onto the server.

Note: In some configurations, the server certificate is the default certificate, rather than a certificate signed by a trusted CA. In that case, you can add that certificate to an allowlist, which explicitly adds that certificate to the custom keystore, as described in [Certificate allowlists and blocklists](#).

What to do next

If you know that a certificate can no longer be trusted, you can add it to a blocklist in the custom keystore. For more information, see [Certificate allowlists and blocklists](#).

Configuring certificate mirroring

Certificate mirroring allows an External S-TAP to automatically generate copies of client and server key pairs from an existing signing key pair. Use certificate mirroring to provide mutual authentication for sites with more than one client certificate.

Before you begin

Before you load the certificate and signing key pair into Kubernetes, make sure that your system meets the following prerequisites.

- Make sure that the signing key pair is a certificate and private key pair with the following attributes:

```
[ v3_intermediate_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid(always,issuer)
basicConstraints = critical, CA:true, pathlen:0
keyUsage = critical, digitalSignature, cRLSign, keyCertSign
```

These attributes mark the key pair as a certificate authority (CA), an issuer, and an entity with the ability to sign new key pairs. The attributes for your environment might vary, but the key pair must be able to sign new key pairs that are trusted by both the client and backend.

- You need a functional Kubernetes deployment cluster that meets the following requirements:
 - You have an accessible Docker repository (public or private) with the External S-TAP image.
 - The database backend is configured with TLS.
 - You have a trusted signing certificate and key pair in a Kubernetes secret. For more information, see the Kubernetes documentation about secrets.
 - All of the trusted certificates are stored in a bundle within the Kubernetes secret.

About this task

Use certificate mirroring to support monitoring services that use certificate-based mutual authentication, since client certificates are duplicated and provided to the backend service.

In a certificate mirroring scenario, you provide a signing key pair to External S-TAP. Guardium® uses the signing key pair to sign new key pairs that are based on the certificates that are sent by the client and backend. To the client and the server, it appears as if they are directly connected to each other over TLS.

To ensure that only trusted certificates are mirrored, you can concatenate all of the trusted certificates into a PEM-formatted bundle, and set the STAP CONFIG PROXY DISCONNECT ON INVALID CERTIFICATE configuration parameter to 1.

These precautions cause any connections that provide an untrusted certificate to be disconnected and not mirrored.

Procedure

1. Load the signing certificate and private key (in PEM format) into a Kubernetes secret.
 2. Load the Kubernetes secret into the External S-TAP container as a file.
 3. In the Kubernetes deployment yaml file, provide the file path in the External S-TAP configuration parameter STAP_CONFIG_ROOT_CA_PEM_PATH.

Example

The following example shows a sample Kubernetes yaml file with the External S-TAP deployment with certificate mirroring enabled.

```
apiVersion: v1
kind: Secret
metadata:
  # This secret needs to contain the base 64 encoded signing certificate and key in pem format
  name: signing-key
  namespace: default
data:
  # below is a vim command for loading the certificate and key into the yaml
  # :r !cat intermediate.cert.pem intermediate.key.pem | base64 | tr -d '\n'
  signing-key.pem: ""
---
apiVersion: v1
kind: Secret
metadata:
  # This secret needs to contain the bundle of trusted certificates
  name: ca-chain
  namespace: default
data:
  # :r !cat ca-chain.cert.pem | base64 | tr -d '\n'
  ca-chain.pem: ""
---
apiVersion: apps/v1
kind: Deployment
metadata:
  name: postgres-etap
  labels:
    app: postgres-etap
spec:
  replicas: 1
  selector:
    matchLabels:
      component: postgres-etap
      tier: backend
  template:
    metadata:
      labels:
        component: postgres-etap
        tier: backend
    spec:
```

```

volumes:
- name: dshm
  emptyDir:
    medium: Memory
    sizeLimit: 756Mi
# Bring in the secrets for the signing key and trusted bundle
- name: etap-signing
  secret:
    secretName: signing-key
- name: etap-ca-chain
  secret:
    secretName: ca-chain
containers:
- imagePullPolicy: Always
  name: postgres-etap
  image: ibmcom/guardium_external_s-tap:v11_4_0
  env:
    - name: STAP_CONFIG_TAP_TAP_IP
      value: "NULL"
    - name: STAP_CONFIG_PROXY_GROUP_UUID
      value: "postgres-etap-group"
    - name: STAP_CONFIG_PROXY_GROUP_MEMBER_COUNT
      value: "1"
    - name: STAP_CONFIG_PROXY_DB_HOST
      value: "postgres.example.com"
    - name: STAP_CONFIG_PROXY_NUM_WORKERS
      value: "1"
    - name: STAP_CONFIG_PROXY_PROXY_PROTOCOL
      value: "0"
# Disconnect on valid certificate ensures that ETAP will only mirror trusted certificates
- name: STAP_CONFIG_PROXY_DISCONNECT_ON_INVALID_CERTIFICATE
  value: "1"
- name: STAP_CONFIG_PROXY_NOTIFY_ON_INVALID_CERTIFICATE
  value: "0"
# Change this value to match the port the backend is listening on
- name: STAP_CONFIG_DB_0_REAL_DB_PORT
  value: "31194"
# Port this pod should listen on
- name: STAP_CONFIG_PROXY_LISTEN_PORT
  value: "5432"
- name: STAP_CONFIG_PROXY_DEBUG
  value: "0"
# Change this value to match the proxy secret returned during S-TAP certificate request creation.
- name: STAP_CONFIG_DB_0_DB_TYPE
  value: "pgsql"
# Change this value to match the ip address of the Guardium collector where the certificate is registered.
- name: STAP_CONFIG_SQLGUARD_0_SQLGUARD_IP
  value: "sqlguard.example.com"
# Location in the container of the signing certificate and key
- name: STAP_CONFIG_ROOT_CA_PEM_PATH
  value: "/etc/ssl/sign/signing-key.pem"
# Location in the container of the bundle of trusted certificates
- name: STAP_CONFIG_CUSTOM_CA_BUNDLE_PEM_PATH
  value: "/etc/ssl/ca/ca-chain.pem"
- name: container
  value: docker
ports:
- containerPort: 5432
volumeMounts:
- mountPath: /dev/shm
  name: dshm
# Mount the secrets in their appropriate locations
- mountPath: /etc/ssl/ca/
  name: etap-ca-chain
- mountPath: /etc/ssl/sign/
  name: etap-signing
```
apiVersion: v1
kind: Service
metadata:
 name: postgres-etap-service
spec:
 type: LoadBalancer
 selector:
 component: "postgres-etap"
 tier: "backend"
 ports:
 - protocol: TCP
 port: 5432 # Port that clients will connect to
 targetPort: 5432
 name: postgres-etap
```

```

Preparing SSL certificates for client applications

To use client applications with External S-TAP, you might need to update the database client by specifying a new database endpoint and port from External S-TAP.

About this task

To deploy an External S-TAP, you need to prepare a private key (proxy.Key) and certificate (proxy.pem) that is signed by the trusted root certificate (rootCA.pem). You can store the certificate in a Guardium® collector, a persistent volume, or Kubernetes secret. If the database uses TLS/SSL, then you also need to distribute the root certificate (rootCA.pem) to the database client.

Procedure

1. Set up the database client.

You might need to update the database client by specifying a new database endpoint and port from External S-TAP. To enable TLS or SSL on connection, specify the following driver setting in the jdbc url connection string for your database:

- SQL Server - sqlserver (encrypt=true)
- PostgreSQL - postgresql (ssl=on)
- MongoDB - mongodb (tls=true)

2. Configure certificates for Java™ applications.

You can configure access to certificates in your application with the following mechanisms:

- The Java virtual machine (JVM) truststore and JVM keystore.
 - A client-specific truststore and keystore.
- a. Configure the JVM truststore by adding the following parameters,
- javax.net.ssl.trustStore - The path to a truststore that contains the certificate of the signing authority.
 - javax.net.ssl.trustStorePassword - The password to access the truststore that is defined in javax.net.ssl.trustStore.
- b. Run the following keytool commands to import the rootCA.pem certificate to the keystore,

```
keytool -importcert -trustcacerts -file <path to CA file that External S-TAP uses>
-keystore <path to trust store> -storepass <password>
```

- c. Configure the JVM keystore. Use an application that initiates TLS or SSL requests to set the following JVM system properties to ensure that the client presents a TLS/SSL certificate to the database server,
- javax.net.ssl.keyStore - The path to a keystore that contains the client's TLS/SSL certificates.
 - javax.net.ssl.keyStorePassword - The password to access the keystore that is defined in javax.net.ssl.keyStore.

3. Create a keystore by using the keytool or OpenSSL. From the keytool, enter the following command,

```
keytool -keystore clientkeystore -genkey -alias client
```

What to do next

Note: By default, the driver ensures that the hostname included in the server's TLS/SSL certificates matches the provided hostnames. You can choose to disable hostname and server certificate verification, then you do not need to create a client-side certificate. To disable these verification methods, set the connection URL property trustServerCertificate=true.

By default, the driver ensures that the hostname included in the server's TLS/SSL certificates matches the provided hostnames. If you need to disable hostname verification or server certificate verification, change the driver properties.

To restrict your application to use the TLS 1.x protocol only, set the jdk.tls.client.protocols system property to TLSv1.x.

Deploying External S-TAP with an operator

Use Kubernetes with a computer assisted software engineering (CASE) operator to deploy your External S-TAPs. You can deploy External S-TAP as a stand-alone service, similar to installing and running the External S-TAP from Cloud Pak for Data v 4.0.

Before you begin

Ensure that the cluster meets the minimum requirements for installing External S-TAP. For more information, see [External S-TAP requirements](#). Verify that a cluster administrator completed the following tasks:

1. The project where you plan to install External S-TAP exists.
2. Optional but recommended, export the following environment variables:

Note: Make sure that the CASE_VERSION is correct for your implementation. Run the following command to check the CASE versions:

```
>oc ibm-pak list --case-name ibm-estap
* Versions listing for ibm-estap *
CASE      Version   App Version
ibm-estap  1.0.0    1.0.0
ibm-estap  1.0.1    1.0.1
ibm-estap  1.1.0    1.1.0
ibm-estap  1.1.1    1.1.1
ibm-estap  1.1.2    1.1.2
```

The following example shows CASE_VERSION=1.1.1. However, make sure to use the version that matches your app version.

```
# Set the working directory to use
export WORKDIR=$HOME
# Set the IBM-PAK working directory
export IBMPAK_HOME=$WORKDIR
# Set the name of the CASE
export CASE_NAME=ibm-estap
# Set the version of the CASE
export CASE_VERSION=1.1.1
# Set the namespace of the Cloud Pak for Data instance
export CPD_NAMESPACE=cpd-inst-01
```

3. Use the following command to download the CASE:

```
pushd $WORKDIR; oc ibm-pak get $CASE_NAME --version $CASE_VERSION; popd
```

4. For environments that use a private container registry, such as air-gapped environments, the External S-TAP software images are mirrored to the private container registry. For more information, see [Mirroring images to your private container registry](#).
5. The cluster is configured to pull the External S-TAP software images. For more information, see [Configuring the cluster to pull images](#).
6. The Guardium External S-TAP catalog source exists. For more information, see [Creating catalog sources](#).
7. The Guardium External S-TAP operator subscription exists. For more information, see [Creating operator subscriptions](#).

If these tasks are not complete, the External S-TAP installation will fail

About this task

After you have completed the previous steps, you can deploy the External S-TAP container. For details about deploying the External S-TAP container, see [Enabling the External S-TAP provisioning UI](#).

- [Mirroring images to your private container registry](#)
Guardium External S-TAP images are accessible from the IBM Cloud Container Registry. In many situations, Guardium recommends that you mirror the necessary software images from the IBM Cloud Container Registry to a private container registry.
- [Configuring the cluster to pull images](#)
If you are using a private registry, you need to update your cluster configuration to ensure that your cluster can pull External S-TAP software images. If you are using IBM Cloud Container Registry, you can skip this step.
- [Creating catalog sources](#)
If you are using a private container registry, you must create the catalog source for each service that you plan to install.
- [Creating operator subscriptions](#)
An operator subscription tells the cluster where to install a given operator and gives information about the operator to Operator Lifecycle Manager (OLM).
- [Enabling the External S-TAP provisioning UI](#)
After all of the prerequisites are met, a project administrator can enable provisioning UI for the External S-TAP container.
- [Provisioning an instance of External S-TAP](#)
Before you can use the External S-TAP service, you must provision an instance service. Each provisioned instance corresponds to a certain cloud database that you want to proxy through Guardium Data Protection.

Mirroring images to your private container registry

Guardium® External S-TAP images are accessible from the IBM Cloud® Container Registry. In many situations, Guardium recommends that you mirror the necessary software images from the IBM Cloud Container Registry to a private container registry.

Important: If your cluster is air-gapped (also called an offline or disconnected cluster), then you must mirror the necessary images to your private container registry. Even if your environment is not air-gapped, consider using a private container registry if you want to:

- Run security scans against the software images before you install them on your cluster.
- Ensure that you have the same images available for multiple deployments, such as development or test environments and production environments.

IBM suggests that you pull images directly from the IBM Cloud Container Registry if your cluster is not air-gapped, your network is extremely reliable, and latency is not a concern. However, if your system does not meet all of those requirements, mirror the images to a private container registry for predictable and reliable performance.

Define the environment variables

The first step is to define the environment variables that describe your private registry. For example:

```
export REGISTRY_IMAGE=docker.io/library/registry:2.7
export REGISTRY_HOST=`uname -n`
export REGISTRY_PORT=5000
export REGISTRY_USERNAME="user"
export REGISTRY_PASSWORD="pass"
```

Create a private registry (optional)

An example of how to create an insecure registry on a bastion node follows.

1. Define the environment variables for the registry that you want to create. For example:

```
REGISTRY_IMAGE=docker.io/library/registry:2.7
export REGISTRY_NAME=docker-registry
export REGISTRY_HOST=`uname -n`
export REGISTRY_PORT=5000
export REGISTRY_DIR=/root/registry
export REGISTRY_TLS_CA_SUBJECT="/C=US/ST=New York/L=Armonk/O=IBM/CN=IBM CA"
export REGISTRY_TLS_CERT_SUBJECT="/C=US/ST=New York/L=Armonk/O=IBM/CN=$REGISTRY_HOST"
export REGISTRY_TLS_CERT_SUBJECT_ALT_NAME="subjectAltName=IP:127.0.0.1,DNS:localhost,DNS:$REGISTRY_HOST"
export REGISTRY_USERNAME="user"
export REGISTRY_PASSWORD="pass"
```

2. Prepare the persistent storage:

```
mkdir -p $REGISTRY_DIR
mkdir -p $REGISTRY_DIR/data
mkdir -p $REGISTRY_DIR/auth
mkdir -p $REGISTRY_DIR/certs
echo $REGISTRY_HOST > $REGISTRY_DIR/hostname
```

3. Configure authentication:

```
dnf install httpd-tools
htpasswd -bBc $REGISTRY_DIR/auth/htpasswd $REGISTRY_USERNAME $REGISTRY_PASSWORD
```

4. Generate the certificate:

```
openssl genrsa -out ${REGISTRY_DIR}/certs/ca.key 4096
openssl req -new -x509 -days 365 -sha256 -subj "${REGISTRY_TLS_CA_SUBJECT}" -key "${REGISTRY_DIR}/certs/ca.key" -out
"${REGISTRY_DIR}/certs/ca.crt"
openssl req -newkey rsa:4096 -nodes -subj "${REGISTRY_TLS_CERT_SUBJECT}" -keyout "${REGISTRY_DIR}/certs/server.key" -out
"${REGISTRY_DIR}/certs/server.csr"
openssl x509 -req -days 365 -sha256 -extfile <(printf "${REGISTRY_TLS_CERT_SUBJECT_ALT_NAME}") -CAcreateserial -CA
"${REGISTRY_DIR}/certs/ca.crt" -CAkey "${REGISTRY_DIR}/certs/ca.key" -in "${REGISTRY_DIR}/certs/server.csr" -out
"${REGISTRY_DIR}/certs/server.crt"
```

5. Start the registry:

```
podman run --name "${REGISTRY_NAME}" -p ${REGISTRY_PORT}:5000 --restart=always \
-v ${REGISTRY_DIR}/data:/var/lib/registry:z \
-v ${REGISTRY_DIR}/auth:/auth:z \
-v ${REGISTRY_DIR}/certs:/certs:z \
-e REGISTRY_AUTH=htpasswd \
-e REGISTRY_AUTH_HTPASSWD_REALM=RegistryRealm \
-e REGISTRY_AUTH_HTPASSWD_PATH=/auth/htpasswd \
-e REGISTRY_HTTP_TLS_CERTIFICATE=/certs/server.crt \
-e REGISTRY_HTTP_TLS_KEY=/certs/server.key \
-d ${REGISTRY_IMAGE}
```

6. Store the certificate for the registry in a configmap in the openshift-config namespace:

```
oc create configmap registry-cas -n openshift-config --from-
file=${REGISTRY_NAME}.${REGISTRY_PORT}=${REGISTRY_DIR}/certs/server.crt
```

7. Add the new configmap to the trust store for the OpenShift cluster:

```
oc patch image.config.openshift.io/cluster --patch '{"spec": {"additionalTrustedCA": {"name": "registry-cas"}}}' --type=merge
```

Cloud Pak for Data images

IBM Cloud Pak software uses the following prefixes to identify images. These publicly available images are provided by IBM. The images do not require an entitlement key to download.

- `cp.icr.io/cpopen` - IBM Cloud Pak® for Data images.
- `icr.io/guardium-insight` - IBM® Guardium Insights images.

Ensure that:

- Your private container registry is configured to allow these prefixes.
- The credentials that you use to push images to the private container registry can push images with these prefixes.

Methods for mirroring images

There are several ways that you can mirror images from the IBM Cloud Container Registry to your private container registry. Choose the most appropriate method for your environment:

| Method | Description | Connected clusters | Air-gapped clusters |
|-------------------------|--|--------------------|---------------------|
| Portable compute device | Example: A laptop that you can move behind your firewall is a portable compute device.
High-level process using a portable compute device: <ol style="list-style-type: none">1. Create an intermediary container registry on a portable compute device that is connected to the internet.2. From the portable compute device, mirror images from the IBM Cloud Container Registry to the intermediary container registry.3. Bring the device behind your firewall and mirror the images from the intermediary container registry to the private container registry that is accessible from the Red Hat OpenShift Container Platform cluster. | | ✓ |
| File transfer | Example: You can either use a portable storage device, such as a USB drive, or use <code>scp</code> or <code>sftp</code> to move images behind your firewall.
High-level process using a file transfer: <ol style="list-style-type: none">1. Create an intermediary container registry. If you are using a portable storage device, create the intermediary container registry on the storage device.2. From a workstation that can connect to the internet and the intermediary container registry, mirror the images from the IBM Cloud Container Registry to the intermediary container registry.3. Move the files and or the storage device behind your firewall.4. Set up a workstation behind the firewall to mirror the images to the private container registry that is accessible from the Red Hat OpenShift Container Platform cluster. | | ✓ |
| Bastion node | Example: A server with access to both the public internet and the private container registry that is accessible from the Red Hat OpenShift Container Platform cluster.
If you use a bastion node, replicate the images from the IBM Cloud Container Registry to the private container registry that is accessible from the Red Hat OpenShift Container Platform cluster. | ✓ | ✓ |

Pull and mirror images

Note: **Best practice:** You can run the commands in this task exactly as written if you set up environment variables that are described in step 2 of [Deploying External S-TAP with an operator](#). Run the environment variable script before you run the commands in this task.

Take the following steps to mirror the images to a private registry.

1. Generate the mirror image list from a machine that can access the IBM Cloud Registry (icr.io):

```
pushd $WORKDIR; oc ibm-pak generate mirror-manifests $CASE_NAME MIRROR --version $CASE_VERSION; popd
```

2. Download the images:

a. Create a directory to store the mirrored images:

```
mkdir -p $WORKDIR/.ibm-pak/data/mirror/export
```

b. Download the images to the local directory:

```
pushd $WORKDIR ; while read MAPPING; do SOURCE="docker://`echo $MAPPING | cut -d '=' -f1`"; DEST="dir:$WORKDIR/.ibm-pak/data/mirror/export/`echo $MAPPING | cut -d '=' -f2 | sed "s/^.*\///"; echo "Copying $SOURCE -> $DEST" ; skopeo copy $SOURCE $DEST --remove-signatures --src-tls-verify=false --dest-tls-verify=false ; done < $WORKDIR/.ibm-pak/data/mirror/$CASE_NAME/$CASE_VERSION/images-mapping.txt ; popd
```

3. From a system that has access to the private container registry, take the following steps:

a. Copy the .ibm-pak directory to a machine with access to the internal registry, then continue to the next step on that machine.

b. Push the images to the private repository:

```
pushd $WORKDIR ; while read MAPPING; do DEST="docker://$REGISTRY_HOST:$REGISTRY_PORT/`echo $MAPPING | cut -d '=' -f2 | sed "s/^.*\///"; echo "Copying $SOURCE -> $DEST" ; skopeo copy $SOURCE $DEST --remove-signatures --src-tls-verify=false --dest-tls-verify=false --dest-creds "$REGISTRY_USERNAME:$REGISTRY_PASSWORD" ; done < $WORKDIR/.ibm-pak/data/mirror/$CASE_NAME/$CASE_VERSION/images-mapping.txt ; popd
```

What's next

After you create the container and store it in the registry, you need to configure the global pull secret, as described in [Configuring the cluster to pull images](#).

Configuring the cluster to pull images

If you are using a private registry, you need to update your cluster configuration to ensure that your cluster can pull External S-TAP software images. If you are using IBM Cloud® Container Registry, you can skip this step.

Permissions you need for this task

You must be a cluster administrator.

When you need to complete this task

You must complete this task the first time you install an External S-TAP.

Note: **Best practice:** You can run the commands in this task exactly as written if you set up environment variables that are described in step 2 of [Deploying External S-TAP with an operator](#). Run the environment variable script before you run the commands in this task.

Procedure

You only need to configure a global pull-secret and update the image source content policy only if your cluster pulls images from a private container registry.

The global image pull-secret must contain the credentials of an account that can *pull* images from the registry.

Important: When you change the global image pull-secret, each node in the cluster is *automatically* restarted so that the Machine Config Operator can apply the changes. This restart process happens one node at a time. The cluster will wait for a node to restart before starting the process on the next node. In some situations, it takes more than 30 minutes for all of the nodes to be restarted. During this process, you might notice that resources are temporarily unavailable.

If your deployment is on cloud, you must *manually* reload the worker nodes in your cluster for the changes to take effect.

1. Configure the global image pull-secret:

a. Confirm that the following installation variables are set based on the private container registry that OpenShift is going to pull from:

```
echo $REGISTRY_HOST
echo $REGISTRY_PORT
echo $REGISTRY_USERNAME
echo $REGISTRY_PASSWORD
```

b. Create an environment variable that points to a temporary directory on your workstation. For example:

```
export WORK_ROOT=$HOME/temp/work
```

c. Download the pull-secret for the cluster:

```
oc get secret/pull-secret
-n openshift-config
--template='{{index .data ".dockerconfigjson" | base64decode}}' > $WORKDIR/global_pull_secret.cfg
```

d. Store the registry credentials to the pull-secret config file:

```
oc registry login --registry="$REGISTRY_HOST:$REGISTRY_PORT" --auth-basic="$REGISTRY_USERNAME:$REGISTRY_PASSWORD" --
to=$WORKDIR/global_pull_secret.cfg
```

e. Update the global pull-secret with the new data:

```
oc set data secret/pull-secret
-n openshift-config
--from-file==$WORKDIR/global_pull_secret.cfg
```

f. Watch the machine config pool (MCP) status to see when all worker nodes have been updated to use the new pull-secret data:

```
watch oc get mcp
```

2. Edit the image content source policy:

a. Configure the cluster to pull from the mirror registry. Use the following command to open the source policy:

```
oc edit imagecontentsourcepolicy
```

Make changes to imagecontentsourcepolicy as needed for your system:

```
apiVersion: v1
kind: List
items:
- apiVersion: operator.openshift.io/v1alpha1
  kind: ImageContentSourcePolicy
  metadata:
    name: cloud-pak-for-data-cpfs-mirror
  spec:
    repositoryDigestMirrors:
      - mirrors:
          - $REGISTRY_HOST:$REGISTRY_PORT/cpopen
            source: icr.io/cpopen
      - mirrors:
          - $REGISTRY_HOST:$REGISTRY_PORT/guardium-insights
            source: icr.io/guardium-insights
```

b. Run the imagecontentsourcepolicy policy and wait until all of the nodes are updated. You can use the following command to track the progress:

```
watch oc get mcp
```

What's next

After you update the global pull-secret and push the images to the private repository, you can create your catalog sources as described in [Creating catalog sources](#).

Creating catalog sources

If you are using a private container registry, you must create the catalog source for each service that you plan to install.

Permissions you need for this task

You must be a cluster administrator.

When you need to complete this task

You must create the catalog sources for any of the software that you plan to install.

Note: **Best practice:** You can run the commands in this task exactly as written if you set up environment variables that are described in step 2 of [Deploying External S-TAP with an operator](#). Run the environment variable script before you run the commands in this task.

Run the following commands to install the catalog source:

1. Install the catalog source:

```
pushd $WORKDIR; oc ibm-pak launch $CASE_NAME --version $CASE_VERSION
--action install-catalog --inventory ibmEtapSetup --namespace openshift-marketplace
--args "--inputDir $WORKDIR/.ibm-pak/data/cases/$CASE_NAME/$CASE_VERSION"; popd
```

2. Verify the installation with the following command:

```
oc get catalogsource -n openshift-marketplace ibm-estap-catalog
-o jsonpath='{.status.connectionState.lastObservedState} {"\n"}'
```

Verify that the system returns **READY**. If it returns **CONNECTING**, wait until **READY** is returned.

Now that you've created the required catalog sources for your environment, you are ready to complete [Creating operator subscriptions](#).

Creating operator subscriptions

An operator subscription tells the cluster where to install a given operator and gives information about the operator to Operator Lifecycle Manager (OLM).

Before you begin

Note: You can run the commands in this task exactly as written if you set up environment variables for your installation. Run the environment variable script before you run the commands in this task.

Creating an operator subscription for External S-TAP

First, use the following commands to install the operator subscription:

```
pushd $WORKDIR; oc ibm-pak launch $CASE_NAME
--version $CASE_VERSION --action install-operator --inventory ibmEtapSetup --namespace
$CPD_NAMESPACE --args "--inputDir $WORKDIR/.ibm-pak/data/cases/$CASE_NAME/$CASE_VERSION"; popd
```

Then, take the following steps to verify that the operator is created:

1. Verify that the CSV for your CASE version is installed. For example:

```
ibm-estap-v1.1.1
```

```
oc get sub -n $CPD_NAMESPACE ibm-estap-catalog-subscription -o jsonpath='{.status.installedCSV} {"\n"}'
```

Note: Make sure that you check the correct CASE version. For more information about finding the correct CASE version, see [Before you begin](#).

- Verify that the CSV install strategy completed with no errors:

```
oc get csv -n $CPD_NAMESPACE $CASE_NAME.v$CASE_VERSION -o jsonpath='{ .status.phase } : { .status.message } {"\n"}'
```

- Verify that the deployment is ready by ensuring that one or more replicas are available:

```
oc get deployments -n $CPD_NAMESPACE -l olm.owner="$CASE_NAME.v$CASE_VERSION" -o jsonpath=".items[0].status.availableReplicas {'\n'}"
```

Important: If you create the Guardium External S-TAP operator with the manual install plan (installPlanApproval: Manual), a cluster administrator must approve the update request for ibm-estap-operator.

After you create and test the operator subscriptions, you can deploy the External S-TAP container as described in [Enabling the External S-TAP provisioning UI](#).

Enabling the External S-TAP provisioning UI

After all of the prerequisites are met, a project administrator can enable provisioning UI for the External S-TAP container.

Before you begin

Ensure that the cluster meets the minimum requirements for installing External S-TAP. For details, see [External S-TAP requirements](#). Specifically, verify that a cluster administrator completed the following tasks:

- The project where you plan to install External S-TAP exists.
- You have completed the tasks in [Deploying External S-TAP with an operator](#).

If these tasks are not complete, the External S-TAP deployment will fail.

About this task

You must be an administrator of the OpenShift® project (Kubernetes namespace) where you will deploy External S-TAP.

External S-TAP uses the following storage classes. If you don't use these storage classes on your cluster, ensure that you have a storage class with an equivalent definition:

- OpenShift Container Storage: ocs-storagecluster-cephfs
- NFS: managed-nfs-storage
- Portworx: portworx-shared-gp3

Procedure

- Log in to Red Hat® OpenShift Container Platform as a user with sufficient permissions to complete the task:

```
oc login OpenShift_URL:port
```

- Create the EstapServiceCPDAddOn custom resource to install External S-TAP. Follow the appropriate guidance for your environment.

```
cat | oc apply -f - << EOF
apiVersion: estap.ibm.com/v1
kind: EstapServiceCPDAddOn
metadata:
  labels:
    app.kubernetes.io/instance: ibm-estap
    app.kubernetes.io/managed-by: ibm-estap
    app.kubernetes.io/name: ibm-estap
  name: enable-ui
  namespace: $CPD_NAMESPACE
spec:
  cloudpakfordata: true
  description: External S-TAP CPD AddOn
  global:
    docker_registry_prefix: icr.io/guardium-insights
  license:
    accept: true
  version: $CASE_VERSION
EOF
```

- Run the following command to verify that the status of the EstapServiceCPDAddOn custom resource is **Completed**:

```
oc get -n $CPD_NAMESPACE EstapServiceCPDAddOn/enable-ui -o jsonpath='{.status.estapStatus} {"\n"}'
```

If it returns **InProgress**, wait until the system returns **Completed**.

What to do next

After you create the custom resource, you can provision the External S-TAP, as described in [Provisioning an instance of External S-TAP](#).

Provisioning an instance of External S-TAP

Before you can use the External S-TAP service, you must provision an instance service. Each provisioned instance corresponds to a certain cloud database that you want to proxy through Guardium® Data Protection.

Before you begin

Ensure that the External S-TAP service meets all of the prerequisites, as described in [Deploying External S-TAP with an operator](#).

About this task

Any IBM Cloud Pak® for Data user with Create service instances permission can provision an instance of the External S-TAP service. Each provisioned instance corresponds to a certain cloud database that you want to proxy through Guardium.

Procedure

1. Open the New service instance for External S-TAP page.
 - a. From the IBM Cloud Pak for Data home page, browse to Services > Services catalog. Then find and select Guardium External S-TAP under Data sources.
 - b. Select the Guardium External S-TAP text or logo to open the description page, and then click Provision instance to open the New service instance for the External S-TAP service.

The New service instance page contains a number of tabs. For each instance of an External S-TAP you want to provision, enter the information for each page, and then click Next to continue.

 2. From the Instance details tab, provide the following information and then click Next.
 - Name - Required. A name for this External S-TAP instance.
 - Namespace - Required. Select the Kubernetes namespace for this instance.
 - Description
 3. From the Storage tab, enter the following details for persistent storage.
 - Use existing storage - If a persistent volume claim (PVC) is available, then select this option and specify the PVC Claim name to use for storage
 - Create new storage - To create new storage, select the Storage class from the list and use the Size in GB slider to specify the size. The default is 1 GB.
 4. Under the General tab, enter information about the deployment and image.
 - Worker threads - Specify the number of threads for each External S-TAP container. You can specify up the number of cores available on the Kubernetes worker nodes.
 - Scaling type - Determine whether you want to use a default scaling type or customize the scaling. If you select predefined, you can select the following options:
 - Deployment size - Select a deployment size or use the default. Changing the deployment size determines the number of pods.
 - Pod memory size - The initial size of the pod's memory limit. Use the default, unless your deployment experiences *out of memory* issues. In that case, change the Pod memory size to *large*.
 - If you select custom, specify the following information:
 - Replicas - Use the slider to select the number of replicas of this instance to create. The default is 2.
 - CPU request - Default = 500m
 - Memory request - Default = 512Mi
 - CPU limit - Default = 500m
 - Memory limit - Default = 512Mi
 - For more information, see [Scaling services](#).
 - NodePort - Specify either random (the default) or specific. For specific, use the slider to select a port number on which to create the NodePort. When you deploy External S-TAP, the deployment creates a load balancer that uses the specified NodePort.
Note: If you select a port that is already in use, the deployment fails. Use kubectl to determine available ports.
 - Service account name - A service account provides an identity for processes that run in a Kubernetes pod. Specify the service account name that your site uses to create Kubernetes pods. If you don't have service account name, use *default*.
 - Registry path - Required. Specify the registry path that is accessible from the namespace that contains the External S-TAP image.
 - Image selection method - Specify the method to select the External S-TAP. Enter the following information:
 - Image label - Required. Specify the label of the External S-TAP image in the registry.
 - Hash or Tag - Depending on the selection method that you choose, specify either the image tag or the hash of the image name. Use Hash to specify a specific External S-TAP container image.
 - Use Tag to specify a class of External S-TAP images that you can use. For example, specify *v11.4.0* to pull the latest *v11.4* image. Make sure that the image tag you specify is intended to be deployed with the installed assembly version.
 - Image pull policy - Defaults to *IfNotPresent*.
5. From the Database and proxy tab, provide the following information.
 - Enter information for the back-end database service parameters:
 - Database host - Required. Specify the hostname or IP of the database instance for which the External S-TAP will monitor client connections.
 - Database port - Required. Use the slider to select a port for which the specified database is listening for client connections.
 - Database type - Required. Specify the type of database to monitor. The string must be one of the documented allowable database type strings for IBM Guardium External S-TAP. For information about supported data sources, see [IBM Guardium System Requirements and Supported Platforms](#) and select the System Requirements document for your Guardium version.
 - Debug - Enables debug logging for troubleshooting. Leave debug set to *0 (off)* except when debugging and troubleshooting. When debug is on, decrypted traffic might be stored in the logs and the additional logging might impact the performance of the External S-TAP.
 - Enter information for the general proxy parameters:
 - Proxy secret token - Specify the key for the token that is retrieved from the Guardium collector that is stored as the Kubernetes secret (from the General page). The proxy secret token is required only if you are retrieving or signing certificates from a Guardium collector. For more information, see [Managing certificates](#).

- Proxy group UUID - Specify a unique identifier to group replicas together in the Guardium appliance. If you do not specify the UUID, a UUID is randomly generated.
- Proxy protocol expected - When enabled, Proxy protocol expected tells the External S-TAP to expect a proxy protocol v1 packet at the beginning of each client connection. If the packet is not present, then the connection fails. External S-TAP removes the proxy protocol packet from the data stream before it relays the connection to the back-end service.
- Disconnect on invalid certificate - When enabled, disconnect the External S-TAP from the client or server if the certificate is invalid.
- Notify on invalid certificate - When enabled, send an alert that a client or server with an invalid certificate has attempted to contact the External S-TAP.
- Internal container listen port - Select the port on which the External S-TAP listens inside the container.
Note: This port is exposed by the load-balancing service and its associated NodePort. Note that port 8080 is exposed for an HTTP health check, but is not exposed by a service.
- Enter information for the proxy certificate signing request (CSR) parameters. This information is required only if you are retrieving or signing certificates from a Guardium collector. For more information, see [Managing certificates](#).
 - CSR Common Name - The common name for the CSR.
 - CSR Country - The country or region for the CSR.
 - CSR Province - The state or province for the CSR.
 - CSR City - The city or locality for the CSR.
 - CSR Organization - The organization or business name for the CSR.
 - Key length - Specify the key length for the CSR key.

6. From the Collector tab, provide information about the primary Guardium collector and up to nine secondary collectors.

For the primary collector, provide the following information:

- Primary Guardium collector host - Specify the hostname or IP of the Guardium appliance to which the External S-TAPs will connect.
- Primary Guardium collector port - Select the base port on which this Guardium appliance accepts UNIX protocol traffic.
- Primary Guardium collector connection pool size - Specify the number of auxiliary threads that the External S-TAP creates to send data to the Guardium appliance.
- Primary Guardium collector number of main threads - Specify the number of main threads created by External S-TAP to communicate with the Guardium appliance.
Main threads are used to participate in load balancing with options 1 and 4. When multiple main threads are available, the Guardium S-TAP connects multiple times to the same collector when threading the S-TAPs intercepted traffic read end. This is a shortcut for specifying the same collector multiple times as secondary collectors.
Note: Set the number of main threads to greater than 1 only when the collector has the capacity for the extra connections.
- Participate in load balancing with Guardium collectors - Select one of the following load-balancing options for External S-TAP.
 - 0 - No load balancing (default). Traffic is sent to one alive server. The primary server has highest priority.
 - 1 - Split sessions between collectors. Traffic is split between servers.
 - 2 - Duplicate traffic to all collectors. Traffic is sent to all servers.
 - 3 - Hardware load balancing with a load balancer such as F5. S-TAP sends traffic to the load balancer, which forwards it to one of the collectors in the pool.
 - 4 - Split sessions between collectors (multi-threading). Traffic is managed (and split) by multiple S-TAP threads.

Each External S-TAP instance can support up to nine additional collectors. If you start to add information for a secondary collector, the framework for the next collector displays. Leave the Secondary Guardium collector host field blank to ignore the collector.

Select All can control to allow all appliances to change the S-TAP configuration. If not selected, only the primary collector can make changes.

- Secondary Guardium collector host - A secondary hostname or IP of a Guardium appliance to which the External S-TAPs can connect. If you leave this field blank, the secondary collector is ignored.
- Secondary Guardium collector port - Select the base port on which this Guardium appliance accepts UNIX protocol traffic.
- Secondary Guardium collector connection pool size - Specify the number of auxiliary threads that the External S-TAP creates to send data to the Guardium appliance.
- Secondary Guardium collector number of main threads - Specify the number of main threads created by External S-TAP to communicate with the Guardium appliance.

7. Use the Probes and Limits tab to configure liveness and readiness probes along with some other options. In general, you do not need to change any of these options.

- Liveness probe options:
 - Probe command - The name of the script that determines whether the container is considered *live*.
 - Initial delay - Enter the time (in seconds) to wait before running the probe. The minimum is 1 and the maximum is 60.
 - Period - Select the time (in seconds) between probe runs (default = 10). The minimum is 1 and the maximum is 600.
 - Failure threshold - Number of failed attempts before stopping (default = 4). The minimum is 1 and the maximum is 10.
- Readiness probe options:
 - Probe command - The name of the script that determines whether the container is considered *ready*.
 - Initial delay - Enter the time (in seconds) to wait before running the probe. The minimum is 1 and the maximum is 60.
 - Period - Select the time (in seconds) between probe runs (default = 5). The minimum is 1 and the maximum is 600.
 - Failure threshold - Number of failed attempts before stopping (default = 5). The minimum is 1 and the maximum is 10.
- Advanced External S-TAP feature options:
 - Override server IP - If you enter a hostname or server IP, override the server IP that is recorded for intercepted traffic in the Guardium appliance with this value.
 - SQLGuard Certificate Common Name - If you provide a common name (CN), the External S-TAP checks the specified CN against the certificate for the Guardium appliance before the External S-TAP connects. If the CN does not match, the External S-TAP cannot communicate with the Guardium appliance.
 - Guardium certificate authority path - Enter the path to the CA certificate that the External S-TAP uses to verify the connection to the Guardium appliance.
 - Number of packets within which to be required to have detected SSL - Specify whether to look for SSL within a session, as follows:
 - -1 - Detect SSL at any point during a session.
 - 0 - Do not attempt to detect SSL.
 - Any integer greater than 0 - Attempt to detect SSL within the specified number of packets per session.

8. From the Summary page, review all of your settings, and then click Create to create this External S-TAP instance.

Results

From the IBM Cloud Pak for Data console, you can now configure and use External S-TAPs to monitor your data with Guardium.

What to do next

After you provision an External S-TAP instance, add a connection from your database to the External S-TAPs. You can connect to any target database supported by Guardium External S-TAP. For more information about connecting to data sources, see [Connecting to data sources](#). For information about supported data sources, see [IBM Guardium System Requirements and Supported Platforms](#) and select the System Requirements document for your Guardium version.

Deploying External S-TAP with Helm

Use Kubernetes with Helm to automate your External S-TAPs deployment.

Before you begin

Before you use Helm, take the following steps:

- Make sure that Git and Kubernetes are installed in your environment.
- Download and unpack Helm. For more information, see [Installing Helm](#) from the [Helm Docs](#) website.
- Gather the following information to use during installation:
 - DB host endpoint IP/address - The database hostname or IP address.
 - DB host endpoint port - The database host port number.
 - DB host endpoint type - The database type. For more information about supported data sources, see [System requirements](#).
 - Guardium appliance IP/address - The Guardium® collector hostname or IP address.

Procedure

1. Install Helm. On Linux®, run the following commands:

```
curl -fsSL -o get_helm.sh https://raw.githubusercontent.com/helm/helm/master/scripts/get-helm-3
chmod 700 get_helm.sh
./get_helm.sh
```

2. In Git, clone the External S-TAP Helm charts:

```
git clone https://github.com/IBM/Guardium_External_S-TAP
cd Guardium_External_S-TAP/charts
```

3. From the /charts directory, open the overrides_example.yaml file.

4. Search for required parameters in overrides_example.yaml and enter the appropriate values for your site. Parameters are described in the overrides_example.yaml file.

5. Based on your environment, determine how to install the certificate for your site. Uncomment the lines for the method that you select, as follows:

- To install External S-TAP with a default certificate, uncomment the following lines:

```
#secret: "estap-secret"
#secretWriterServiceAccountName: "estap-secret-writer"
```

- To install External S-TAP with a certificate that is stored in the collector, uncomment the following line:

```
#secret: estap-token
```

- To install External S-TAP with a certificate stored in a Kubernetes secret, uncomment the following line:

```
#secret: "estap-secret"
```

Tip: To use a certificate stored in a Kubernetes secret, create the Kubernetes secret by using one of the following methods:

- `kubectl create secret generic <secret-name> --from-literal=estap-token=<TOKEN>`
 - Or
- ```
kubectl create secret tls <secret-name> --key="your-certificate.key" --cert="your-certificate.crt"
```

If needed, use the following command to import the ca.pem file from the secret to the production environment, as follows:

```
kubectl get secret/estap-secret template- {{ 'print (index .data "ca.pem")' | base64 -d}}
```

Make sure that all the parameters are correct for your environment. For example, make sure that the Container image tag references your current Guardium version.

When you are done, save the overrides\_example.yaml file.

6. Run one of the following commands to either install or upgrade the Helm chart:

- To install the Helm chart:

```
helm install -f overrides_example.yaml my-estap-deployment estap
```

- To upgrade an existing Helm chart:

```
helm upgrade -f overrides_example.yaml my-estap-deployment estap
```

where,

- *my-estap-deployment* is the name for this deployment. Specify the name in the Estap Settings section of the yaml file.
- *estap* is the name of the External S-TAP Helm chart.

## What to do next

---

The External S-TAP is now available for use. View and manage the External S-TAP from Guardium. For more information, see [Edit External S-TAP group tab](#). You can now delete the Helm installation files by using the **helm delete** command to make sure that all the necessary files are properly removed. For example,

```
helm delete my-estap-deployment
```

where *my-estap-deployment* is the name of the deployment to delete.

## Deploying External S-TAP from the Guardium UI

If your site uses Kubernetes, you can deploy an External S-TAP directly from Guardium®.

### About this task

Before you can deploy an External S-TAP from Kubernetes, you need to:

1. Create a Kubernetes admin user.
2. Retrieve the Kubernetes cluster access token.
3. Retrieve the Kubernetes control plane URL.
4. Create the registry key for your cluster.
5. Ensure that any SSL-enabled collectors have valid SSL certificates.

Save the cluster access token, the Master URL, and the registry key. You need to enter them into the Kubernetes or Docker tabs of the Deploy External S-TAP window. For more information, see [Deploy External S-TAP window](#).

Note: For **Google Cloud deployments only**: If you plan to deploy the External S-TAP from the Guardium GUI, make sure that the IAM user has the following permissions: `container.clusterRoleBindings.create` and `container.clusterRoles.bind`.

These permissions allow the IAM user to add the cluster user and create tokens for GUI deployment.

Without these permissions, the IAM user can still deploy with Kubernetes by using the templates. For more information about generating and using the templates, see [Deploy External S-TAP window](#).

## Procedure

1. Create a Kubernetes admin user from kubectl (the Kubernetes command-line interface):
  - a. Create a yaml file that contains the following information. For this example, the yaml file is named `admin-service-account.yaml` where `admin-name` is the name of your administrative user:

```
apiVersion: v1
kind: ServiceAccount
metadata:
 name: <admin-name>
 namespace: kube-system

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
 name: <admin-name>
roleRef:
 apiGroup: rbac.authorization.k8s.io
 kind: ClusterRole
 name: cluster-admin
subjects:
- kind: ServiceAccount
 name: <admin-name>
 namespace: kube-system
```

- b. Run the following command from kubectl to create the admin user:

```
$kubectl apply -f admin-service-account.yaml
```

2. Retrieve the Kubernetes cluster access token (also called the secret):

```
$kubectl -n kube-system describe secret $(kubectl -n kube-system get secret | grep <admin-name> | awk '{print $1}')
```

Enter the returned token in the Token field of the Kubernetes tab.

3. Retrieve the Kubernetes control plane URL.

Run **kubectl cluster-info** to find the name of the Kubernetes control plane URL. For example:

```
$kubectl cluster-info
Kubernetes control plane is running at https://azureaks01-dns-e1234567e.hcp.centralus.azmk8s.io:443
. . .
```

Enter the returned URL in the Kubernetes control plane URL field of the Kubernetes tab.

4. Create the registry key, which is called the secret in Kubernetes.

Run the following command to create the registry key, where the `<regcred>` is the secret for your registry:

```
$kubectl create secret docker-registry <regcred> \
--docker-server=$DOCKER_REGISTRY_SERVER \
--docker-username=$DOCKER_USER \
--docker-password=$DOCKER_PASSWORD \
--docker-email=$DOCKER_EMAIL
```

Enter the returned secret in the Registry key field of the Docker tab.

5. Make sure that each SSL-enabled collector on which you deploy an External S-TAP has a valid SSL certificate, as described in [SSL certificates for External S-TAP](#).

## What to do next

---

After you complete these tasks, you can deploy a new External S-TAP directly from Guardium. Kubernetes automatically manages the Docker container and balancing the load.

For more information, see [The External S-TAP user interface](#) and the [Deploy External S-TAP window](#)

## Deploying External S-TAP manually

Deploy an External S-TAP with Docker and the External S-TAP scripts.

After you have the signed SSL certificates, you can deploy the External S-TAP. To deploy an External S-TAP without Kubernetes, take the following steps:

- Download the Docker container as described in [Download the Docker container](#).
- Prepare the deployment script (and load balancer script, if you are using it) as described in [External S-TAP deployment scripts](#).
- After you deploy the External S-TAP, you can view and manage it from the External S-TAP instances page as described in [The External S-TAP user interface](#).

- [Download the Docker container](#)

To deploy a Guardium External S-TAP monitor, you first need to download the IBM Guardium External S-TAP container from the IBM Cloud Container Registry (icr.io). Deploy the container onto the machine (real, virtual, or cloud) that serves as the External S-TAP host.

- [External S-TAP deployment scripts](#)

Before you can run a Guardium External S-TAP container on your system, you need to prepare and run one or two deployment scripts.

## Related concepts

---

- [SSL certificates for External S-TAP](#)

## Download the Docker container

To deploy a Guardium® External S-TAP monitor, you first need to download the IBM® Guardium External S-TAP container from the IBM Cloud Container Registry (icr.io). Deploy the container onto the machine (real, virtual, or cloud) that serves as the External S-TAP host.

## Before you begin

---

1. Make sure that a Linux® environment is available for External S-TAP host. For the External S-TAP, Docker must be installed and running under Linux.
2. For SSL-enabled sites, make sure that you have with the appropriate security certificates as described in [SSL certificates for External S-TAP](#). If your environment is not SSL-enabled, you can skip this step.

## Procedure

---

1. If your site does not provide Docker, install Docker on the External S-TAP host. For more information, see [Get Docker](#).

2. Use `skopeo` to list the available docker tags for Guardium External S-TAP in the IBM Cloud Container Registry ([icr.io](#)). For example:

```
~$ skopeo
list-tags docker://icr.io/guardium-insights/guardium_external_s-tap
```

3. The `skopeo` command returns a list of all available tags for External S-TAP. Find and copy the appropriate docker pull command. For example:

```
myname:~$ skopeo list-tags docker://icr.io/guardium-insights/guardium_external_s-tap
{
 "Repository": "icr.io/guardium-insights/guardium_external_s-tap",
 "Tags": [
 "cpd-3.5-deploy-11.2.1-34",
 ...
 "v11.2.0-deploy-3.5-16",
 ...
 "v11.4.0",
 "v11.4.1",
 ...
 "v11.5.0",
 "v11.5.1"
 "v11.5"
]
}
myname:~$
```

Note: The container for the latest version of each Guardium release is available from the `vX.X` tag for that release. For example, for Guardium 11.5, copy docker pull from the `v11.5` tag.

4. Use the `docker pull` command to download the Docker container into your environment. For example, to pull the latest External S-TAP image,

```
docker pull
icr.io/guardium-insights/guardium_external_s-tap:v11.5
```

For more information about accessing [icr.io](#) and using the `skopeo` command, see <https://www.ibm.com/support/pages/node/6618197>.

To deploy to an internal repository: If your Docker host machine does not have access to the internet, create an internal repository on which to store the Docker containers. One method to create an internal repository is to use multiple steps, for example:

- a. Configure a host to run a local (private) docker registry. For more information, see [Deploy a registry server](#).

- b. Take the following steps on a host that where Docker is installed and that can contact both the local Docker registry and [icr.io](#):

- i. Pull the External S-TAP Docker image from icr.io.

- ii. Push the External S-TAP Docker image to the local Docker registry.
- c. After the image is in the local registry, you can deploy the External S-TAP containers on a host that has access to that registry.

## What to do next

---

After you download the External S-TAP Docker container, you can either deploy the container onto the Docker host machine or, if needed, create the security certificates to help ensure that your system remains secure. For more information, see [External S-TAP deployment scripts](#) or [SSL certificates for External S-TAP](#).

## Related concepts

---

- [SSL certificates for External S-TAP](#)
- [External S-TAP deployment scripts](#)

## External S-TAP deployment scripts

---

Before you can run a Guardium® External S-TAP container on your system, you need to prepare and run one or two deployment scripts.

## Preparing to deploy an External S-TAP

---

At this point, you have an External S-TAP container that is ready to deploy and each collector that is SSL-enabled has a valid SSL certificate. The next steps are to prepare and run the deployment scripts. You can run the scripts from the External S-TAP host or another machine that has access to the External S-TAP host and is running Linux.

1. If you plan to use the load balancing script to create a load balancing solution, you need to prepare the load balancer script. The first step that the deployment script takes is to call the load balancing script. For more information about the load balancer script, see [Load balancer scripts](#).  
Note: Using the load balancing script is recommended, but not required. If your site chooses not to use the load balancing script, make sure that you have another load balancing strategy in place.
2. Run the External S-TAP deployment script, `container_mgmt.sh`, in interactive mode to set the correct options for your site in an iterative fashion.  
Note: If you use persistent storage (see `--persist`), you need to initialize it before running the script. Initializing the persistent storage allows the Docker container to access data. For example,

```
docker run --rm -v my-vol:/persistent busybox /bin/sh -c 'touch /persistent/.initialized && chown -R 1000:1000 /persistent'
```

Note: The deployment and load balancing scripts are available on GitHub at [https://github.com/IBM/Guardium\\_External\\_S-TAP](https://github.com/IBM/Guardium_External_S-TAP). Before you run or modify the scripts, be sure to read the CONTRIBUTOR.md and README.md files.

## External S-TAP deployment example

---

The following example walks through the script that creates the External S-TAP containers in interactive mode:

1. From your Linux® command line, `cd` to the directory where the `container_mgmt.sh` and `lb_interface_nginx.sh` scripts are located.
  2. From the command line, call the `container_mgmt.sh` script, along with the `--state-file` and `--lb-script` parameters, as discussed in [Table 1](#). For example,
- ```
> container_mgmt.sh --state-file sample_state --lb-script lb_interface_nginx.sh
```
- Note: The `--state-file` parameter is always required. The `--lb-script` parameter is required if you are using the load balancing script (recommended). If you do not include `--lb-script`, a warning message displays.
3. At the prompt, specify the action that you want to take, as described in [Table 2](#). Depending on the action you select, the deployment script asks for the information it needs.
 4. For this example, at the `would you like` to prompt, select C and then press Enter to create External S-TAP containers.
Tip: If you are installing External S-TAP on a cloud host, select P to print the list of environment variables that are required to configure your cloud instance for the External S-TAP container.
 5. At the next prompt, `What host do you want to use to host the service containers?` [localhost]
`Non-interactive parameter: --svc-host localhost`
 6. The script echoes the actual parameter name and argument, as shown:

```
What host do you want to use to host the service containers? [localhost]
Non-interactive parameter: --svc-host localhost
```

Tip: Copy each parameter and argument into Notepad or another editor to build up the command line as you determine the required parameters. You can then copy and paste the completed command line into your Linux shell.

7. Continue responding to each prompt.
 - For parameters where you accept the default, press **Enter**.
 - For parameters for which you want to change the default (or which has no default), enter the new value and then press **Enter**.
8. After you successfully run the script, the host computer will `ssh` to the Guardium host and run commands to set up the External S-TAP containers and the load balancer.

When you run the deployment script in an on-premises environment, it creates a cluster of External S-TAP containers. External S-TAPs monitor all transactions, perform TLS decryption and reencryption (if the database is SSL-enabled), and forwards the traffic to the Guardium system. It also (optionally) configures a load balancer that clients can connect to. The load balancer then forwards these connections to one of the External S-TAP containers.

Use [Table 3](#) to determine which parameters you need. The parameters are shown in the order that they are called when you create a new cluster (that is, when you select the `--c` option).

Note: You can rename or edit any of the scripts as required for your installation. Make sure that any changes to one script (such as changing the name of the load balancing script) are propagated to any other scripts that call them. Do not change parameter names.

Required command line parameters

The parameters in [Table 1](#) must be available on the command line. If you do not include **--lb-script** on the command line, you must provide your own load balancing solution. For more information, see [Load balancer scripts](#)

Table 1. Required command line parameters

| Parameter | Meaning |
|---------------------------------|---|
| --state-file
<i>filename</i> | Required. The name of the file in which the state is recorded. For example:

--state-file /ext_stap_state

Note: You must specify the state file in the command line. |
| --lb-script
<i>filename</i> | The name of the load balancer deployment script. If you do not include the name of the load balancer script, you must configure the load balancer separately. For your convenience, two default scripts are available: <ul style="list-style-type: none">• lb_interface_echo.sh - An example script for a generic load balancer (does not work as is).• lb_interface_nginx.sh - An example script to create an NGINX-based load balancer. Note: To use the load balancer script, you must specify the parameter and script name in the command line. |

Selecting the action

Use the parameters in [Table 2](#) to specify the action you want to take each time you run the deployment script. In general, you use this script to create (--c) a cluster of External S-TAP containers. However, you can also use the same script to delete clusters, print the Docker container environment variables, and take other actions, as described in [Table 2](#).

Table 2. External S-TAP action parameters

| Parameter | Meaning |
|-----------|--|
| --ni | Run this script in non-interactive mode. Use interactive mode to set parameters as needed. After the script is set up for your environment, you can run the script in non-interactive mode. |
| --c | Create a cluster. |
| --d | Delete an existing cluster. |
| --e | Enable interception, that is restart intercepting database traffic. Requires the load balancer integration script. This command is generally only used for support and testing purposes. |
| --p | Do not create a cluster, but print the Docker container environment variables. The output is saved in the state file. For hosting in the cloud, use the --p parameter to print the environment variables you need to configure your cloud instance for the External S-TAP container. |
| --r | Remove interception, that is, stop intercepting database traffic. Requires the load balancer integration script. This command is generally only used for support and testing purposes. |
| --u | Upgrade an existing cluster. |
| --z | Clean up zombie instances, that is, stop and delete old containers that are still running on the host. |

Deployment script parameters

The remaining deployment script parameters specify important information for your deployment, such as host names, repository names, and the number of containers to deploy. When you run the script in interactive mode, you are prompted for the value of each parameter. For optional parameters, or to accept default values for required parameters, you can press Enter to continue without entering any information.

Note: The parameters that display depend on the action you select when you call the External S-TAP deployment script.

Table 3. External S-TAP deployment script parameters

| Parameter | Script Question/meaning |
|---------------------------------|--|
| --svc-host <i>host/ip</i> | What host do you want to use to host the service containers?
The host name or IP address of the host or hosts on which to create the containers. Separate multiple host names with a comma.

The default is \$SVC_HOST. |
| --svc-port-range <i>m-n</i> | What is the port range for the exported service port?
The exported port number for the Docker container. You can specify a range of available ports between <i>m-n</i> (inclusive). In this case, the host dynamically determines the port number for each Docker container. For example:

--svc-port-range 6100-6500

The default is 0, which uses the values from:

/proc/sys/net/ipv4/ip_local_port_range |
| --svc-host-user <i>username</i> | What user will be logging in to the host to start the service containers?
The user name of the user who creates containers on the Docker host machine.

The default is the current user, \$SVC_HOST_USER |
| --svc-image <i>image</i> | Enter the hash or tag for the service container image:
The name or hash of the External S-TAP image from Docker. For example:

--svc-image store/ibmcorp/guardium_external_s-tap:v10.6.0 |
| --repo-user <i>username</i> | What is the username to be used if login is required to pull the service container image?
The user name of the user who logs in to the repository from which the External S-TAP Docker image is pulled. |
| --repo-pass <i>password</i> | What is the password for user?
The password for the repo-user user name.

Tip: Before running the deployment script, log in to Docker (on the Docker host machine) with docker login to save your login information to <code>~/.docker/config.json</code> . After you are logged in, you do not need to enter the --repo-user and --repo-pass parameters. |

| Parameter | Script Question/Meaning |
|---------------------------------|--|
| --svc-container-num num | How many service containers would you like to create?
The number of External S-TAP Docker containers to create for this database inspection cluster.

The default is 1. |
| --uuid UUID | Please enter a UUID for this group:
The UUID of the External S-TAP cluster. The default is a random UUID generated from <code>uuidgen</code> . |
| --proxy-num-workers n | Enter the number of workers for each service container of Guardium External S-TAP:
The number of worker threads for the External S-TAP to use. You can set the number of worker threads from the Guardium collector Edit External S-TAP group page after the cluster is created.

The default is 1. |
| --db-host host/ip | Enter the hostname or IP to which the DB the Guardium External S-TAP group will be relaying traffic:
The host name or IP address to the computer where the External S-TAP will forward connections. |
| --db-type string | Enter the type of database for the DB host:
The database type for External S-TAP traffic. You can set the database type from the Guardium collector Edit External S-TAP group page after the cluster is created. Supported databases are listed on the Database tab of the Deploy External S-TAP page. |
| --db-port port | Enter the port for the DB to which the Guardium External S-TAP group will be relaying traffic:
The port number needed to access this cluster. You can set the port number from the Guardium collector Edit X-TAP group page after the cluster is created. |
| override_server_ip/ P address | Enter an IP to override and force the server IP to be reported as (optional and uncommon, leave blank if not needed) |
| --proxy-protocol n | If proxy protocol version 1 is enabled for the DB traffic, enter 1, otherwise enter 0:
Specifies whether the proxy protocol is enabled for the database traffic. For more information, see https://www.haproxy.org/download/1.8/doc/proxy-protocol.txt .

<ul style="list-style-type: none"> • 0 - Not enabled (default). • 1 - Protocol version 1.
If your load balancer supports proxy protocol, the protocol inserts data at the beginning of the connection to share the client's IP address with External S-TAP. With proxy protocol, connections are reported as being from the client to the DB host.

You can change this setting from the Guardium collector Edit External S-TAP group page after the cluster is created. |
| --invalid-cert-disconnect | Do you wish to disconnect the clients if the DB server certificate cannot be verified? (y/n)
If the database server certificate cannot be verified, terminate the client connection. |
| --invalid-cert-notify | Do you wish to log an error message if the DB server certificate cannot be verified? (y/n)
If the database server certificate cannot be verified, continue running and log a warning. |
| --proxy-secret string | Depending on how External S-TAP is configured on your system, you might see one of the following prompts:
If traffic is encrypted and you are generating CSRs on the collector and signing them separately, enter the secret token which will be used to retrieve the key and signed certificate from the Guardium Collector:

. The shared secret string, or token, needed to retrieve keys from the collector for External S-TAP. Run <code>show certificate External S-TAP</code> from the CLI on the Guardium collector to view the token you need to enter for proxy-secret.

Or:

If traffic is encrypted and you have a signing certificate stored on the collector to automatically sign CSRs generated by External S-TAP, enter the Name field for the CSR's CN:

In this case, use the shared secret string to generate a CSR container that is signed by the collector. In this case, the --proxy-csr-name is required.

In either case, --proxy-secret is required if you want to use encrypted External S-TAP traffic. |
| --proxy-csr-name string | If traffic is encrypted and you have a signing certificate stored on the collector to automatically sign CSRs generated by External S-TAP, enter the Name field for the CSR's CN:
Required if you have a signing certificate stored on the collector. Enter a name for the CSR's common name, or CN. |
| --proxy-csr-country string | Enter the Country field for the CSR's CN: |
| --proxy-csr-province string | Enter the Province field for the CSR's CN:
Enter the state or province for the CSR's CN. |
| --proxy-csr-city string | Enter the City field for the CSR's CN: |
| --proxy-csr-organization string | Enter the Organization field for the CSR's CN: |
| --proxy-csr-keylength integer | Enter the length for the CSRs private key:
The length of the CSR private key must be between 2048 and 8192. |
| --sqlguard-ip host/IP address | Enter the hostname or IP of the Guardium Collector:
Required. The collector host name or IP address for External S-TAP to relay decrypted traffic. |
| --sqlguard-cert-cn cn | CN to match when verifying collector certificates. Requires a derived container image with a CA populated at \${GUARDIUM_CA_PATH}
If your site chooses to verify collector certificates, enter the CN (common name) of the collector's certificate. Leave this entry blank to disable verification. For more information, see Verify collector certificates (optional) . |

| Parameter | Script Question/Meaning |
|--------------------------------------|--|
| --participate-in-load-balancing char | <p><code>Participate in load balancing or failover? 0: failover/no_lb, 1) split, 2)</code>
 <code>redundancy, 3) not allowed, 4) threaded:</code>
 <code>. Specify the type of load balancing solution to use.</code></p> <p>You can change this setting from the Guardium collector Edit External S-TAP group page later.</p> |
| --kill-after n | <p><code>Enter the number of seconds to wait before forcefully stopping the old containers (0 is wait 30s, but don't forcefully stop):</code>
 When stopping a container, if the container does not shut down within n seconds, forcefully remove it. The default is to wait 30 seconds but don't force removal.
 Note: This parameter does not display when creating containers.</p> |
| --state-file filename | <p><code>Name of the file in which the state is recorded.</code>
 Required. The name of the state file, for example <code>\". ./cluster_state\"</code>.</p> |
| --envvar environment setting | For support purposes only. |
| --persistent Docker volume | <p><code>Persistent storage source</code>
 The name of a Docker persistent volume. The volume must be accessible and shared between all of the nodes at the same path.
 If needed, change the owner on the host machine directory to the same UID as the UID of the External S-TAP. For example,
 <code>chown -R 1000:1000 <path_to_External_S-TAP_volume></code>
 Note: Be sure to initialize the persistent storage before you run the script.</p> |

- [Load balancer scripts](#)

Guardium External S-TAP requires integration with a load balancer to help provide redundancy to eliminate a single point of failure.

Related concepts

- [Load balancer scripts](#)

Load balancer scripts

Guardium® External S-TAP requires integration with a load balancer to help provide redundancy to eliminate a single point of failure.

Guardium provides two sample load balancer integration scripts that you can use as a base for your own script. The scripts provide a set of functions that are called by the Guardium External S-TAP deployment script to create and manage the load balancer configuration for your environment. In coordination with the load balancer integration script, the load balancer allows you to upgrade External S-TAP instances without impacting traffic between the client and server.

Important: If your site chooses not to use the load balancing script, make sure that you have another load balancing solution in place.

Note: Within the scripts, ignore any line that contains the phrase STATE=. Those lines are for internal use only.

You can use one of the sample scripts as a base, but actual implementation details will vary according to your needs. Both of the sample scripts include the required load balancer functions, which are described in [Table 1](#). Changes will be required to either script to meet your site's needs.

- The lb_interface_nginx.sh sample script provides a sample NGINX-based implementation.
- The lb_interface_echo.sh sample script provides information about a generic implementation and echoes back information about elements in the script.

Important: Do not run the load balancing script directly. Always call the script from the External S-TAP deployment script, with the script name as the first argument , for example, `--lb-script filename` (where `filename` is the name of your load balancing script).

The load balancer is activated when the External S-TAP is deployed.

The functions described in [Table 1](#) are required, and must use the exact function names provided. Change each function as needed to meet your site's requirements.

Table 1. Load balancing script functions

| Function name | Meaning |
|---------------------------------|--|
| lb_import_state() | <p>Takes a state file that is created by the deployment script and builds up the load balancer configuration. The file format is as follows:</p> <pre>Container 1 information Container 2 information ... Container n information</pre> <p>Where each line contains the following information as a comma-separated list:</p> <ul style="list-style-type: none"> • <code>host where container is running</code> • <code>external port on host for container</code> • <code>internal container listen port</code> • <code>listen port on database</code> • <code>container name</code> <p>The lb_import_state function prepares the configuration from the state provided. The state is passed to lb_import_state, which is called once each time the deployment script runs, and always before any other function.</p> |
| lb_redirect_around_containers() | Changes the configuration that is created by lb_import_state to temporarily direct traffic around (rather than through) the Docker containers. Receives two parameters that describe the <code>host</code> and <code>port</code> of the target server. Used to temporarily remove interception by External S-TAP instances for debugging and testing. |
| lb_add_one() | Takes two parameters, the <code>host</code> and <code>port</code> of the External S-TAP Docker container to add. The lb_add_one function uses the configuration that is prepared in lb_import_state to add a container to the configuration. |
| lb_remove_one() | Takes two parameters, the <code>host</code> and <code>port</code> of the External S-TAP Docker container to remove. The lb_remove_one function uses the configuration that is prepared in lb_import_state to remove the container from the configuration. |

| Function name | Meaning |
|----------------------|--|
| lb_apply_config() | Takes no parameters. Applies the current state of the configuration to the load balancer. Can be called multiple times per run of the deployment script. |
| lb_teardown_config() | Takes no parameters. Deactivates the load-balancer. Call this function to remove the External S-TAP containers as part of an uninstall process. |
| lb_cleanup() | Takes no parameters. Performs any cleanup necessary to remove temporary files. Call this function once, and only when you will not call load balancer integration again. |

The External S-TAP user interface

Use the External S-TAP instances page to create, monitor, start, stop, and configure Guardium® External S-TAPs.

Use the External S-TAP instances page to deploy an External S-TAP, check on the status of any currently running External S-TAPs, and to modify certain parameters.

To open the page, browse to `Manage > Activity Monitoring > External S-TAP Control`.

The External S-TAP instances page

The External S-TAP instances page displays all of the currently available External S-TAPs on the current Docker host machine, and provides some tools to help manage them.

From the External S-TAP instances page, you can select the following tools:

- New: Click to deploy a new External S-TAP. For more information, see [Deploy External S-TAP window](#).
- Edit: Select an External S-TAP and click to open the Edit External S-TAP group page. For more information, see [Edit External S-TAP group tab](#).
- Delete: Select one or more stopped External S-TAPs and click to delete them from the Guardium database. You cannot delete a running External S-TAP. If your site uses Kubernetes, deleting the External S-TAP from the UI does not remove it from the Kubernetes cluster. To remove the External S-TAP and all of its underlying structures, delete the External S-TAP deployment and service from the Kubernetes dashboard or by using the `kubectl` command-line interface. For more information, see the Kubernetes documentation.
- Refresh: Click to update your view of the External S-TAP instances page.
- Comment: Select an External S-TAP from the list and then click to display the Comments window. Add a comment for the selected External S-TAP and then click Close to save and close the window. Other users can reply to comments or add their own.
- Actions: Select an External S-TAP on which to perform one of the actions in the list. For more information, see [Actions menu](#).
- Export: From the Export menu, select one of the following options to save current information about the available External S-TAPs:
 - Download as CSV: Save information in an Excel file.
 - Download as PDF: Save information in a PDF file.
- Filter: Enter any string into the Filter text box to exclude External S-TAPs that do not contain the specified string. For example, enter 65 to show only those External S-TAPs that have the number 65 in the host IP address or the Group uuid.

For each External S-TAP, the following information displays:

- External S-TAP group: The name of the External S-TAP cluster. The name is created from the database type and the IP address of the Docker host machine.
- Group uuid: The uid for this cluster. The uid can either be a generated uid or a string that was entered as the uid during deployment.
- Host: The IP address of the Docker host machine.
- Database type: The type of database for this External S-TAP.
- Total members: The total number of containers in this cluster. Each cluster contains both a load balancer and one or more External S-TAP containers.
- Overall status: The status of this External S-TAP cluster.
 - If all of the External S-TAPs are down, the status is red.
 - If at least one External S-TAP is running, the status is green.
- Healthy members: The number of healthy members in this cluster. For a cluster with multiple External S-TAPs, if Total members is different than Healthy members, you know that some of the External S-TAPs are down.
- Collector: The name of the Guardium collector that this External S-TAP is using.

Actions menu

After you select an External S-TAP, you can select any of the following options from the Actions menu:

- Restart: Restarts the S-TAP that runs with this External S-TAP.
- S-TAP logging: From the S-TAP logging window, specify an External S-TAP group, a debug level, as described in [Table 1](#), and a time period for which to monitor S-TAP interaction and save the data to the S-TAP log file.
- Run diagnostics: From the Run diagnostics window, specify an External S-TAP group, a debug level, as described in [Table 1](#), and a time period for which to run the S-TAP diagnostics script. The diagnostics run with the specified debug level and are uploaded to the Guardium collector.
- Revoke ignore: If your installation has the IGNORE STAP SESSION (REVOCABLE) rule set, click Revoke ignore to open the Revoke ignore window. Click Apply for the selected External S-TAP group for the S-TAP to start transmitting data for any sessions that were in an ignore state.
- View details: View and manage details for one or more members of a selected External S-TAP group. If you view the details of an External S-TAP group that contains multiple members, all of the members display.

From the External S-TAP details window, you can take the following actions:

- View details and version information for each member of the selected External S-TAP group.
- Delete one or more inactive containers in the group. Select the containers that you want to delete and click . A confirmation message displays. Click Yes to delete the selected containers.

Note: You can delete only inactive containers.

- View events: View the events for the selected External S-TAP group. For each event, the report identifies the Event type, Event description, Timestamp, and Container (Group uuid). You can filter on any string in the report. For example, to see error messages, enter *ERR* to display only events with an event type of LOG-ERR.
- View deployment: View selected details about this External S-TAP deployment.

The External S-TAP page includes the following tabs.

- [Deploy External S-TAP window](#)

If your site uses Kubernetes to manage clusters, you can install and configure an External S-TAP from the Deploy External S-TAP window.

- [Edit External S-TAP group tab](#)

Use the Edit External S-TAP group tab, to view or change the information about an existing Guardium External S-TAP.

Deploy External S-TAP window

If your site uses Kubernetes to manage clusters, you can install and configure an External S-TAP from the Deploy External S-TAP window.

Deploy External S-TAP window

In the Deploy External S-TAP window, enter the required information in the tabs to deploy a new External S-TAP.

Note: For more information about creating the Master URL, Token, and Registry key, see [Deploying External S-TAP from the Guardium UI](#).

When you are done, click Apply to save your changes or Create templates to generate yaml templates that you can use to manage External S-TAPs from Kubernetes.

When you select Create templates, Guardium generates two files, **service.yaml** and **deployment.yaml**. When you call these files from the Kubernetes command line, Kubernetes can manage persistent storage, load balancing, and other External S-TAP requirements.

Note: To use persistent storage with Kubernetes, make the following changes to Kubernetes and to the **deployment.yaml** file:

1. In Kubernetes, create a persistent volume and a persistent volume claim. For PersistentVolumeClaim, make sure that accessModes is set to *ReadWriteMany* to allow the volume to access all of the parallel containers in the deployment.
2. In the **deployment.yaml** file, add the following information under spec:
 - *containers* includes volumeMounts and the following *mountPath*:

```
  containers:
    volumeMounts:
      - mountPath: "/persistent"
        name: mypd
```

- *volumes* includes the name of the persistent volume and persistent volume claim. For example:

```
  volumes:
    - name: mypd
      persistentVolumeClaim:
        claimName: myclaim
```

3. When you are done, apply the changes from kubectl:

```
kubectl apply -f deployment.yaml
```

4. Finally, make sure that persistent storage is deployed:

```
kubectl get deployment
```

For more information, see the Kubernetes documentation.

The Deploy External S-TAP window displays the following tabs:

- [Kubernetes tab](#)

Enter information required to run External S-TAP from Kubernetes.

- [Volume tab](#)

Specify whether to use an existing Kubernetes persistent volume or create a new persistent volume. After you have created the persistent volume, you can choose to use the volume for other External S-TAPs.

- [Docker tab](#)

Enter the registry key and Docker container location for External S-TAP.

- [Database tab](#)

Enter information about the External S-TAP database.

- [Guardium tab](#)

Enter load balancing and collector options.

- [Certificate tab](#)

Enter information to allow the External S-TAP to manage certificates and certificate signing requests (CSRs).

- [Advanced tab](#)

Enter information about certain External S-TAP advanced parameters.

Kubernetes tab

Enter information required to run External S-TAP from Kubernetes.

Table 1. Kubernetes tab parameters

| Parameter | Default | Meaning |
|-----------|---------|---------|
|-----------|---------|---------|

| Parameter | Default | Meaning |
|------------------------------|--------------|--|
| Cloud provider | | To install a cloud-based External S-TAP with Amazon (AWS), IBM (IBM Cloud), or Microsoft (Azure), select a cloud provider. To use an External S-TAP with an on-premises database, leave Cloud provider blank. For more information about deploying to IBM Cloud, see Step deploy_kubernetes.html#deploy_extap_kubernetes_ibm_cloud_deploy of Deploying External S-TAP from the Guardium UI . |
| Use internal load balancer | Not selected | If selected, adds an annotation to the service to set an internal load balancer for the selected cloud provider. |
| Kubernetes control plane URL | | Required. Established when you provision the Kubernetes cluster.
Note: If the Kubernetes control plane URL does not point to a cloud provider, you need to ensure that a load-balancing solution is available. |
| Authentication token | | Required. The Kubernetes cluster access token. |
| Deployment name | | Required. A user-defined name. The name can contain only lowercase alphanumeric characters and a dash (-). The name must start and end with an alphanumeric character (for example 'my-name', or 'philly-58'). |
| Namespace | default | Required. Kubernetes provides a default namespace. Specify <i>default</i> unless you created a namespace for your Kubernetes cluster. For OpenShift, namespace is the same as the project name. |

Volume tab

Specify whether to use an existing Kubernetes persistent volume or create a new persistent volume. After you have created the persistent volume, you can choose to use the volume for other External S-TAPs.

Table 1. Volume tab parameters

| Parameter | Default | Meaning |
|--------------------------------------|---------------|--|
| Use existing persistent volume claim | | If you already created a Kubernetes persistent volume, you can specify the persistent volume claim. |
| Create persistent volume claim | | Create a new Kubernetes persistent volume. If you select this option, then specify the storage and access mode for the volume that you create. |
| Claim name | | The name of the persistent volume claim. |
| Storage | | The amount of storage for this volume. Specify at least 500 mebibytes (MiB). |
| Access mode | ReadWriteMany | The access mode for this persistent volume. The access mode must be <i>ReadWriteMany</i> . |

Docker tab

Enter the registry key and Docker container location for External S-TAP.

Table 1. Docker tab parameters

| Parameter | Default | Meaning |
|------------------------|---------------------------------------|--|
| Registry key | | Required. The registry key, which is also called the Kubernetes cluster <i>Secret</i> . After you create it, you can find the Registry key (the <i>Secret</i>) with the command:
<code>kubectl get secret</code> |
| External S-TAP version | | The version of the External S-TAP you are using. Select whether your External S-TAP is from 11.3 or earlier or 11.4 or later. |
| Location | store/ibmcorp/guardium_external_s-tap | Required. The download location of your Docker image. |
| Tag | | Required. The Docker image tag used for the download. |

Database tab

Enter information about the External S-TAP database.

Table 1. Database tab parameters

| Parameter | Default | Meaning |
|---------------|---------|---|
| Database type | | The database for this External S-TAP. Select a database from the list or leave this field blank. If you leave the field blank, you can specify the database later in the Database type field on the Edit External S-TAP group Inspection engine tab . |
| Database port | | The port on the database host on which the External S-TAP is listening. |
| Database host | | The name or IP address of the database host that is being monitored by this External S-TAP cluster. You can change the name to monitor a different database. |

Guardium tab

Enter load balancing and collector options.

Table 1. Guardium tab parameters

| Parameter | Default | Meaning |
|-------------------|---------|---|
| Collector IP | | The IP address of the Guardium® collector. The collector IP is read-only. |
| Load balancing | 0 | Select an option: <ul style="list-style-type: none"> 0: No load balancing (default). Traffic is sent to one alive server. The primary server has highest priority. 1: Split sessions between collectors. Traffic is split between servers. 2: Duplicate traffic to all collectors. Traffic is sent to all servers. 3: Grid mode. The S-TAP communicates to the collector through a load balancer. |
| Add new collector | | If you select a load-balancing option greater than 0, the  icon becomes available. Click  to add up to 10 Guardium collectors. Change the collector information from the Edit External S-TAP group Collector tab . |

Certificate tab

Enter information to allow the External S-TAP to manage certificates and certificate signing requests (CSRs).

If you select Use CSR to generate certificate, then External S-TAP can automatically generate certificates as needed.

Table 1. Certificate tab parameters

| Parameter | Default | Meaning |
|---------------------------------|--------------|--|
| Certificate storage secret | estap-secret | The Kubernetes secret that contains the token that is used to deploy the External S-TAP. |
| Service account token secret | | The name of the token secret in the namespace where you deploy the External S-TAP. |
| Collector certificate token | | Required for SSL-encrypted traffic. The token, or secret, from the certificate alias. |
| Use CSR to generate certificate | | Select to have the CSR generate on demand External S-TAP certificates. |
| Common Name | | Required. The common name for the CSR. |
| Country/Region | | The country or region for the CSR. |
| State/Province | | The state or region for the CSR. |
| City/Locality | | The city or locality for the CSR. |
| Organization | | The organization or business name for the CSR. |
| Key Length | 2048 | Select the key length for the CSR key. |

Related tasks

- [Configure on-demand certificate generation](#)
- [Manually create a certificate signing request](#)

Advanced tab

Enter information about certain External S-TAP advanced parameters.

The pod security context parameters allow you to use External S-TAP when Kubernetes Pod Security Policies are enabled. The parameters help ensure that the pod user has access to files and mounted volumes. For more information, see the Kubernetes Pod Security Policies documentation.

Table 1. Advanced tab parameters

| Parameter | Default | Meaning |
|------------------------------|---------|--|
| Member count | | The number of External S-TAP Docker containers to create for this database inspection cluster. In general, you don't need more than four containers per cluster. |
| Worker threads | 1 | The number of threads used by each External S-TAP in the cluster. |
| Verify collector certificate | | Select to have any S-TAPs verify the collector's certificate before the collector connects to the S-TAP. Use this feature, along with block lists and allow lists, to strictly control access between the Guardium® collector and the External S-TAP. |
| Collector CN | | If you select Verify collector certificate, enter the common name (CN) of the collector to use in Collector CN, or enter a regular expression to specify a set of allowable collectors.
For more information about Regular Expressions, see Regular Expressions . |
| Override server IP | | Enter a default server IP address to use for all recorded traffic. |
| runAsUser | 1000 | The UID for the processes within the pod containers. If the user is not 1000, then GID 0 must be a valid group for the user. |
| fsGroup | 1000 | The file system group. Enter the GID for filesystem mounts in the containers of the Pod. The fsGroup is added to the pod's supplementalGroups parameter.
The default is 1000, but make sure that you specify a number that works with your policy. |

Edit External S-TAP group tab

Use the Edit External S-TAP group tab, to view or change the information about an existing Guardium® External S-TAP.

The Edit External S-TAP group tab

From the Edit External S-TAP group tab, you can view or change information about existing External S-TAPs. When you select an External S-TAP to edit, the name of the External S-TAP group displays at the top of the tab. You can change the name of the External S-TAP group from External S-TAP group name.

The Edit External S-TAP group tab includes tabs that you can use to change or view properties for the selected External S-TAP group.

External S-TAP tab

The External S-TAP tab allows you to view or change the information that is described in [Table 1](#).

Table 1. External S-TAP tab

| Parameter | Default | Meaning |
|------------------------|---------|---|
| Group uuid | | The uid for this cluster. A read-only parameter. |
| Member count | | The number of External S-TAPs in this cluster. A read-only parameter. |
| Database host | | The name of the database host that is being monitored by this External S-TAP cluster. You can change the name to monitor a different database. |
| Listen port | | The port on the database host on which the External S-TAP is listening. |
| Debug | 0 | Set the debugging level for this External S-TAP. The debug levels are as follows: <ul style="list-style-type: none"> • 0: No debug (the default) • 1: Configuration debug. Creates logs related to configuration and statistics. • 2: Packet digest. Read and write some actions for each packet. • 3: Extended packet digest. Includes information such as connection lifecycle, open, close, or TLS handshake logs, and some per connection logs. • 4: Full verbose debug. Includes all logs and a partial payload dump. |
| Worker threads | 1 | The number of threads used by each External S-TAP in the cluster. |
| Proxy protocol | 0 | Provide support for the load balancer proxy protocol, if it is enabled. For example, for an NGNIX load balancing solution, add proxy_protocol on to the /etc/nginx/nginx.conf configuration file and then enable Proxy protocol in this tab. |
| On invalid certificate | | Specify actions to take if the SSL certificate is not valid. You can choose to disconnect the External S-TAP from the server, notify the user that a server with an invalid certificate has attempted to contact the External S-TAP, or both.. |

Edit External S-TAP group also includes the following tabs:

- [TAP tab](#)

External S-TAPs are designed to use S-TAPs. From the TAP tab, you can set a number of S-TAP-related parameters.

- [Inspection engine tab](#)

From the Inspection engine tab, you can view or change the parameters related to the Guardium inspection engine.

- [Collector tab](#)

From the Collector tab, you can add, edit, or remove a Guardium collector.

- [Firewall tab](#)

From the Firewall tab, you can configure the Guardium firewall for an External S-TAP. Using the Guardium firewall can slow performance and might cause other issues. Guardium suggests that you use the firewall feature only when necessary.

TAP tab

External S-TAPs are designed to use S-TAPs. From the TAP tab, you can set a number of S-TAP-related parameters.

From the TAP tab, you can set a number of S-TAP-related parameters.

For the query rewrite (QRW) parameters,

- Make sure that QRW force watch and QRW force unwatch are not configured with the same IP ranges.
- In addition, these options are valid only when QRW installed is selected and QRW default state is set to 1.

The following caveats apply for QRW:

- QRW with External S-TAP works with the following databases:
 - Db2 (Linux and UNIX)
 - Microsoft SQL
 - Oracle
- You cannot deploy External S-TAP with QRW enabled. Deploy the External S-TAP first, and then enable QRW from the GUI.

For more information about the query rewrite parameters, see [Linux-UNIX: Query rewrite parameters](#).

Table 1. TAP tab

| Parameter | Default | Meaning |
|-----------------|-------------|---|
| All can control | Not checked | For configurations with multiple collectors, specifies whether all collectors can change the configuration or only the primary collector can make changes. The default allows only the primary collector to make changes. |
| Messages | Not checked | Turn remote and syslog messages on or off: <ul style="list-style-type: none"> • Remote: When selected, sends messages to the active Guardium® host. • Syslog: When selected, records system messages in the syslog. |

| Parameter | Default | Meaning |
|-----------------------------|---------|--|
| Load balancing | | Select a load balancing option: <ul style="list-style-type: none"> 0: No load balancing (default). Traffic is sent to one alive server. The primary server has highest priority. 1: Split sessions between collectors. Traffic is split between servers. 2: Duplicate traffic to all collectors. Traffic is sent to all servers. 4: Split sessions between collectors (multi-threading). Traffic is managed (and split) by multiple S-TAP threads. |
| Managed units | 1 | The number of managed units (MUs) to request from the load balancer |
| Compression level | 1 | Select the level of data compression between the S-TAP and the collector. Choose a compression level between 1 (none) to 9 (highest). |
| QRW force unwatch | | Client IPs addresses and masks (for example, 192.168.0.0/192.168.0.10) to exclude from watching.
Click  to add additional IP addresses and masks. |
| QRW force watch | | Client IP addresses and masks (for example, 192.168.0.0/32) to automatically watch .
Click  to add additional IP addresses and masks. |
| QRW default state | | Sets the query rewrite activation trigger. Must be 0 if Firewall default state (on the Firewall tab) is set to 1. Valid values: <ul style="list-style-type: none"> 0: QRW is activated per session when triggered by a rule in the installed policy. 1: QRW is activated for every session regardless of the installed policy. |
| QRW installed | | Enables or disables the Dynamic Data Masking for Databases feature. When set to 0, all other QRW parameters are ignored. |
| Load balancer node affinity | | For enterprise load balancing, specifies whether the S-TAP connects to more than one managed unit.
For more information, see Load balancer node affinity . |

Inspection engine tab

From the Inspection engine tab, you can view or change the parameters related to the Guardium inspection engine.

From the Inspection engine tab, you can view or change the parameters that are described in [Table 1](#).

Table 1. Inspection engine tab

| Parameter | Default | Meaning |
|------------------|---------|---|
| Database type | | The type of database for this External S-TAP. If you did not select a database when you deployed the External S-TAP, you can specify it here. If you selected a database earlier, the field displays the selected database type and is read-only. |
| Database port | | The port on which the database is listening. |
| Networks | Blank | Identify specific clients to monitor by IP address. Specify a begin and end range of IP addresses to monitor. If blank, all clients are monitored.
Note: You can specify either Networks or Exclude networks, but not both. |
| Exclude networks | Blank | Identify specific clients to exclude from monitoring. Specify a begin and end range of IP addresses to exclude. If blank, all clients are monitored. |
| Priority count | 20 | Specify the number of packets of a session to set as high priority. The first <i>number of packets</i> are sent to the high priority queue in the sniffer. The range is from 0 (off) to 50. |

Collector tab

From the Collector tab, you can add, edit, or remove a Guardium® collector.

- To add a collector, click the  icon to display the Add new collector window. In this window, enter the information described in [Table 1](#) and then click Save to save the new collector.

Table 1. Collector tab

| Parameter | Default | Meaning |
|----------------|---------|--|
| Guardium host | | The name of the Guardium collector you want to add. |
| Main threads | 1 | When you select load balancing methods 1 or 4 to split load balancing, the number of open main connections between the S-TAP and a server. For more information, see TAP tab . |
| Pool size | 1 | The number of open data connections between an S-TAP and a sniffer process on a server. |
| Set as primary | | If you have multiple collectors, select a collector to serve as the primary collector. |
| Filter | | Enter any string into the Filter text box to exclude collectors that do not contain the specified string. |

- To edit an existing collector, select the collector and then click  icon to display the Edit collector window. From this window, you can view the collector name and change the Main threads and Pool size, as described in [Table 1](#).

Make any changes that you want, and click Save to save your changes or Cancel to exit without saving.

- To delete an existing collector, select the collector and click the  icon. The collector is deleted.

Note: If you accidentally delete a collector, click Cancel to close the Edit External S-TAP group window without saving your changes.

Firewall tab

From the Firewall tab, you can configure the Guardium® firewall for an External S-TAP. Using the Guardium firewall can slow performance and might cause other issues. Guardium suggests that you use the firewall feature only when necessary.

The Firewall tab parameters are based on the Linux-UNIX firewall parameters for S-TAPs. For more information, see [Linux-UNIX: Firewall parameters](#). For more information about Guardium policies and the firewall, see [Blocking rule actions](#).

Table 1. Firewall tab

| Parameter | Default | Meaning |
|------------------------|--------------|--|
| Firewall installed | 0 | Enables or disables the firewall feature. Valid values: <ul style="list-style-type: none"> • 0: Disables the firewall. • 1: Enables the firewall. |
| Firewall timeout | 10 (seconds) | Time, in seconds, to wait for a verdict from the Guardium system. If the firewall times out, the Firewall fail close value determines whether to block or allow the connection. The value can be any integer value. |
| Firewall default state | 0 | Sets the default state for the firewall. Valid values: <ul style="list-style-type: none"> • 0: The firewall is activated per session when triggered by a rule in the installed policy. • 1: Watch all traffic for firewall policy violations. • 2: Watch all traffic for firewall policy violations for the initial priority_count packets. The External S-TAP watches the initial part of every new session to your database. Setting the default state to 2 is useful when you have session-based policies, firewall rules based on the user, or some other information that is passed early in the session. It limits the impact of firewall on the performance. Instead of watching every bit of the session (Firewall default state=1) and waiting for an UNWATCH verdict, the External S-TAP unwatches automatically if no WATCH or DROP is sent. |
| Firewall fail close | 0 | The action to take when the verdict cannot be set by the policy rules, for example, if Firewall timeout expires. <ul style="list-style-type: none"> • If the check box is selected, the connection is blocked. • If not selected, the connection goes through. |
| Firewall force watch | | A comma-separated list of IP/mask values.
If Firewall default state is set to 0 (off), then Firewall force watch specifies the network address or mask of the IP addresses that you want the firewall to watch, overriding the default. |
| Firewall force unwatch | | A comma-separated list of IP/mask values.
If Firewall default state is set to 1 (on), then Firewall force unwatch specifies the network address or mask of the IP addresses that you want the firewall to ignore, overriding the default. |

Related reference

- [Linux-UNIX: Firewall parameters](#)

Best practices for using External S-TAPs with on-premises databases

To use External S-TAPs with on-premises databases, you need to take a few steps to prepare both your database and the External S-TAP. Examples are shown using PostgreSQL.

To use an External S-TAP solution with an on-premises database, make sure that:

- All remote traffic can be directed through the External S-TAPs by using TCP/IP.
- Determine whether to use mutual authentication for the on-premises databases. If you do use mutual authentication, local traffic to the database is allowed only through an unencrypted named pipe protocol, which is monitored by an S-TAP. For more information, see [Manage certificates for mutual authentication](#).
- Your site uses TCP/IP to configure the firewall to block both local and remote traffic except from the External S-TAP host. For more information, see [Set up a firewall on Linux](#).

Prepare the deployment

Gather the following information about your database:

- The database IP address or host name and ports.
- Determine whether your database is SSL-enabled (encrypted).
- Determine whether your database is using mutual authentication.

Set up the solution to monitor databases

To monitor databases with an External S-TAP, you need both an S-TAP and an External S-TAP. The S-TAP is required to monitor local traffic, and the External S-TAP monitors remote traffic.

To prepare the solution, take the following steps:

1. Install an S-TAP on the database host and add (or modify) an inspection engine to accept local traffic to monitor the local connection to the database. Use an unencrypted named pipe (npipe) for the S-TAP.
Note: When you install an S-TAP to use with an External S-TAP, set the intercept type to `npipe` for each database you want to monitor, as follows:
 - From the GUI, under Inspection Engine, set Intercept Types to `npipe`.
 - From the interactive installer, set intercept_types=`npipe` in the `guard_tap.ini` file.
 For more information about installing an S-TAP, see [Linux-UNIX: Install S-TAP agents installation flow](#).
2. Deploy the External S-TAP to monitor remote connections by using TCP/IP protocol. For more information, see [Inspection engine tab](#) or [External S-TAP deployment scripts](#), depending on your deployment method. Optionally, to use mutual authentication, the root certificates that are used by the External S-TAPs must be the

same as the root certificates for the database.

- Secure your database by setting up the firewall. Make sure that all remote traffic goes through the External S-TAPs.

Manage certificates for mutual authentication

To use the mutual authentication option with External S-TAPs, the External S-TAP certificate must be signed by the same certificate authority (CA) as the host database certificate.

When you create the External S-TAP certificate, the CN (Common Name) parameter is required. For mutual authentication, make sure that the CN of the certificate that is used by the External S-TAP is the same as the External S-TAP host name. In addition, if you use a load balancer, use the same certificate CN as the end point of the load balancer.

Set up a firewall on Linux

Use the following example to configure iptables to prevent direct access to your on-premises database. For the following example:

- The PostgreSQL database listen port is 5432.
- External S-TAPs are installed on 172.17.0.3 and 172.17.0.4.

The following code example configures the iptables to prevent direct access to PostgreSQL:

```
# Reject access to MongoDB container
iptables -I INPUT -p tcp --dport 5432 -j REJECT
# Allow access to MongoDB container from External S-TAP (IP needs to match)
iptables -I INPUT -p tcp --src 172.17.0.3 --dport 5432 -j ACCEPT
iptables -I INPUT -p tcp --src 172.17.0.4 --dport 5432 -j ACCEPT
iptables -I DOCKER-USER -p tcp --src 172.17.0.3 --dport 5432 -j ACCEPT
iptables -I DOCKER-USER -p tcp --src 172.17.0.4 --dport 5432 -j ACCEPT
```

Additional notes about certificates for External S-TAPs

The host parameter of certificate for External S-TAP must match the CN of the certificate that the database client gets in the TLS handshake, that is:

- If the client connects to the server directly, the host parameter must match the CN of the certificate on the PostgreSQL or MySQL server.
- If the client connects to the server via an External S-TAP, set the host parameter to the host of the External S-TAP. Make sure that the CN of the External S-TAP certificate matches the host parameter in the command.
- If the External S-TAP uses a TCP-IP load balancer, set the host parameter to the host or domain name of the load balancer. Make sure that the CN of the External S-TAP certificate matches the host parameter.

PostgreSQL notes

To use PostgreSQL with mutual authentication, make sure that the host parameter that is used by client matches the CN of the certificate of the External S-TAP.

Note: You can use a wildcard to match the certificate CN.

For PostgreSQL, the METHOD field in the pg_hba.conf file controls the client authentication method. External S-TAP supports the following methods:

- trust, trust clientcert=1
- md5, md5 clientcert=1
- password, password clientcert=1

Configuring AWS HA for External S-TAPs

Include External S-TAPs in your existing Amazon AWS high availability (HA), or failover, configuration.

If your site uses Amazon AWS that is configured for high availability (HA), or failover, Guardium® recommends that you include External S-TAPs in your existing HA configuration. Include External S-TAPs in your existing failover scenario by integrating with either Elastic Load Balancer, Route 53, or both. To integrate External S-TAPs in your failover scenario, you can:

- Add multiple External S-TAP instances behind your load balancer for active-active failover.
- Use your DNS server to deploy active-passive failover for External S-TAP instances.

Note: Guardium assumes that your site is already using HA configuration with Amazon AWS. For more information about using an HA configuration with Amazon, see the [Amazon Route 53 Developer Guide](#) (and other Amazon and AWS documentation). Because your configuration is based on your specific requirements, Guardium can provide only general guidance for how to configure HA and failover for your site.

Prerequisites

To use External S-TAPs in an HA environment, the following applications must be deployed inside your AWS service, along with any web services:

- Amazon EC2 and Relational Database Service (RDS).
- AWS Identity and Access Management (IAM): Assign appropriate roles to run Lambda functions.
- Amazon Route 53: Provides domain registration, DNS routing, and health checking.
- Amazon CloudWatch: Monitors services and provides actionable insights and alerts.
- Health Check (AWS ELB): Monitors registered instances to ensure that the load balancer sends requests only to healthy instances.
- Amazon Simple Notification Service (SNS): Provides messaging services between CloudWatch Alarm and Lambda functions.
- Amazon Lambda: A serverless platform that the failover mechanism uses to provide a trigger point to maintain firewall rules.
- AWS Elastic Load Balancing (ELB): Automatically distributes traffic between multiple External S-TAP instances for load balancing and active-active failover. ELB also acts as the entry for the External S-TAP micro service.

Configuring failover for External S-TAP

The following instructions assume that you are familiar with Amazon AWS for HA and failover for other applications.

1. In Route 53, register for a domain name and create health check rules as needed, including checks to monitor CloudWatch alarms.
 - Health check constantly monitors traffic through the External S-TAP.
 - If the failure rate for a health check rule exceeds the configured threshold, health check triggers an alarm or events.
2. Configure SNS and CloudWatch as needed. When an alarm is triggered, CloudWatch alarms and SNS notifications update the DNS record and the access control list rules. In addition, you can set SNS to notify IT or other personnel. In Route53, you can configure CloudWatch to monitor the health checks.
3. In the EC2 Management Console, create and configure a Security Group specifically for the External S-TAP. To provide flexibility in managing firewall rules, Guardium recommends that you also create security groups for the load balancer, PostgreSQL client, and PostgreSQL server domains.
4. Route 53 reroutes the DNS servers when a server fails. The DNS server updates the record according to the status of the alarm. Configure Route 53 to:
 - Create a policy record to route the entry domain to a different domain based on the status of the CloudWatch alarm.
 - In your DNS, find or create the following domains:
 - A domain for the load balancer. For failover, specify this domain as the primary domain. The endpoint for this domain is available from AWS > Amazon RDS > Databases > <your_dbname>.
 - An entry domain of the policy record. Specify this domain as the secondary domain. The DNS name can be found from Amazon EC2 Management Console > Load Balancing > Load Balancers.
 - The DNS of the service endpoint in RDS. The domain name depends on your configuration. For instance, the name might be found in the Amazon Route 53 dashboard under Hosted Zones > Policy Records as the Policy Record DNS Name for the External S-TAP traffic policy.
5. In AWS Lambda, create functions to update the access control list rules. Make sure that your Lambda functions have an IAM rule that has sufficient permissions.

After you add an External S-TAP to your HA configuration, CloudWatch monitors the External S-TAP along with your other applications.

Configuring Google BigQuery for External S-TAPs

Include External S-TAPs in your Google BigQuery configuration for Guardium®.

You can use External S-TAPs to intercept Google BigQuery traffic in three different ways:

- The BigQuery client libraries
- BigQuery JDBC driver from CData Software
- Google Cloud Console

You can deploy External S-TAP for Google BigQuery either with Kubernetes as described in [Deploying External S-TAP from the Guardium UI](#) or with Docker, as described in [Deploying External S-TAP manually](#).

If you use Kubernetes, set the following Kubernetes environment variables for External S-TAP:

- STAP_CONFIG_PROXY_DB_HOST=*bigrquery.googleapis.com*
- STAP_CONFIG_DB_0_REAL_DB_PORT=443
- STAP_CONFIG_DB_0_DB_TYPE=bigrquery

If you use Docker, set the following variables in the deployment script:

- db_host: *bigrquery.googleapis.com*
- db_type: *bigrquery*
- db_port: 443

How you configure Google BigQuery depends on which method you want to use to intercept traffic. Follow the directions for the method you want to use.

Configure the certificate for BigQuery client libraries or CData BigQuery JDBC driver

For either the BigQuery client libraries or the CData BigQuery JDBC driver, you need to take the following steps:

1. Generate a replacement certificate and private key for External S-TAP that meet the following requirements:
 - The key type is RSA.
 - Common Name (CN) - *bigrquery.googleapis.com*
 - Subject Alternative Names (SAN) - *DNS:*.cloud.google.com, DNS:clients6.google.com, DNS:*.clients6.google.com, DNS:bigrquery.googleapis.com*
 - The certificate is signed by a CA key pair.
2. Deploy the certificate and private key. Combine the certificate and private key into a single file and put them into a Docker volume or Kubernetes secret.
 - If you use a Kubernetes cluster, set the External S-TAP `STAP_CONFIG_PROXY_PEM_PATH` environment variable to the path of the file that contains the combined certificate and key inside the container.
 - If you use Docker on a virtual machine, store the certificate and private key by using the “store certificate external_stap_signing” cli command which creates a certificate token for the External S-TAP. For more information, see [Certificate CLI Commands](#).
3. Configure DNS so that the clients you want to monitor get the IP address of the External S-TAP for the following domain names:
 - *bigrquery.googleapis.com*
 - *console.cloud.google.com*
 - *cloudconsole-pa.clients6.google.com*
 - *clients6.google.com*

Note: To test on a local machine, you can use an entry into `/etc/hosts`. For production, Guardium suggests that you use a DNS system (such as BIND 9).

Configure the BigQuery API Client Libraries

To use the Google BigQuery API Client Libraries with External S-TAP, you first need to install the client libraries, as described in the Google Cloud BigQuery documentation. Then, configure the client library to trust the new External S-TAP certificate as well as the certificates that make up the signing chain.

To use the `bq cli` tool, you must append the External S-TAP certificate and signing chain to the `cacerts.txt` file, which you can find in one of the following locations (depending on your python version).

- `/google-cloud-sdk/platform/bq/third_party/httplib2/python3/cacerts.txt`
- `/google-cloud-sdk/platform/bq/third_party/httplib2/python2/cacerts.txt`

Configure the CData BigQuery JDBC driver

If you plan to use the CData BigQuery JDBC driver to connect through External S-TAP, you first need to install and configure the CData BigQuery JDBC driver. For more information, see the CData JDBC Driver for Google BigQuery documentation.

After you configure the CData BigQuery JDBC driver for your project, data set, and OAuth, set the following properties:

- `ProxyAuthScheme=NONE`
- `ProxyPort=443`
- `ProxySSLType=ALWAYS`
- `ProxyServer=` The IP address of your External S-TAP. If not set correctly, the Google BigQuery servers reject the connection with a "handshake failure."
- `SSLServerCert=` The path to the file that contains the External S-TAP certificate and signing chain.

Configuring Google Cloud Console (BigQuery web UI)

To use an External S-TAP to intercept data from the Google Cloud Console, create or select a Google Cloud project.

Note: BigQuery is automatically enabled in Cloud Console projects.

1. Generate a replacement certificate and private key for External S-TAP that meet the following requirements:

- The key type is `ECDSA` with `secp256r1 (prime256v1)`
 - Common Name (CN) - `bigrquery.googleapis.com`.
 - Subject Alternative Names (SAN) - `DNS:*.cloud.google.com, DNS:clients6.google.com, DNS:*.clients6.google.com, DNS:bigrquery.googleapis.com`.
 - The certificate is signed by a CA key pair.
2. Deploy the certificate and private key. Combine the certificate and private key into a single file and put them into a Docker volume or Kubernetes secret.
 - If you use a Kubernetes cluster, set the `External S-TAP_CONFIG_PROXY_PEM_PATH` environment variable to the path of the file that contains the combined certificate and key inside the container.
 - If you use Docker on a virtual machine, store the certificate and private key by using the `store certificate external_stap_signing` cli command which creates a certificate token for the External S-TAP. For more information, see [Certificate CLI Commands](#).
 3. Configure DNS so that the clients you want to monitor get the IP address of the External S-TAP for the following domain names:
 - `bigrquery.googleapis.com`
 - `console.cloud.google.com`
 - `cloudconsole-pa.clients6.google.com`
 - `clients6.google.com`

Note: To test on a local machine, you can use an entry into `/etc/hosts`. For production, Guardium suggests that you use a DNS system (such as BIND 9).

4. Configure the web browser. Make the following changes to the client web browser:

Tip: This example uses the Firefox web browser. For other browsers, the parameters might be slightly different. From Firefox, change the settings from the preference page. Enter `about:config` in the Firefox address bar, and click through the warnings to open the preference page.

- a. When available, the Google BigQuery Cloud Console uses HTTP 2. Since Sniffer does not support HTTP 2, you need to disable HTTP 2 support in the browser to force it to use HTTP 1.1.
 - `network.http.spdy.enabled = false`
 - `network.http.spdy.enabled.http2 = false`

- b. The client web browser needs to trust the External S-TAP certificate and signing chain.
 - `security.osclientcerts.autoload = true`
 - `security.enterprise_roots.enabled = true`

- c. Add the External S-TAP certificate (along with the other certificates in the signing chain) to your browser's trusted certificates.

On Linux, copy the External S-TAP certificate and the rest of the certificates in its signing chain to the following location:

```
/etc/pki/ca-trust/source/anchors/
```

In Windows, take the following steps:

- Break all of the certificates into separate certificate files with a `.crt` file extension.
- Import the certificates into a Windows trusted CA by clicking each certificate file to display an import dialog.
- If the certificate is the root CA, select Trusted root Certificate Authorities. For intermediate certificates, select Intermediate Certificate Authorities.

- d. After the certificates are in place, you need to update the certificate truststores. Run the following command as root:

```
update-ca-trust
```

If your browser is open, you need to close and reopen it.

Troubleshooting External S-TAP issues

Check for solutions if something goes wrong with your External S-TAPs.

The database connection closes unexpectedly

When External S-TAPs are running, you might encounter an infrequent situation in which the database connection closes unexpectedly. In this case, you need to delete the certificate that is associated with the External S-TAP and restart the External S-TAP, as follows:

1. Call `delete_certificate_external_stap` from the Guardium CLI to delete the certificate. This command lists all the available certificates that are associated with External S-TAPs. Select the number that corresponds to the certificate for the associated External S-TAP.
2. Restart the External S-TAP from the UI.

Even without the External S-TAP certificate, the External S-TAP continues to forward traffic to the database.

Database is blocked due to too many connection errors

If your site is using Amazon elastic Kubernetes service (EKS) with Aurora MySQL, you might experience connection errors. In this case, in the Amazon Relational Database Service (RDS) console, set the values for the following instance-level parameters by applying the Parameter Groups to your database instance.

- max_connect_errors=10000
- max_connections = 200

Client IP is not correctly recorded for session

Load balancers and proxies can obscure the IP of the client. This behavior is not unique to External S-TAP and multiple methods are available to address this issue. One straight-forward method is to use a load balancer that can inject a proxy protocol.

Note: Most databases do not accept proxy protocol themselves and if proxy protocol is enabled, External S-TAP cannot accept sessions without proxy protocol. If a proxy protocol packet is expected, the packet must exist. Conversely, if a proxy protocol is not expected, the existence of a packet causes the connection to fail.

External S-TAP consumes and removes the proxy protocol packet from the database stream before it sends the session to the backend service.

In AWS, proxy protocol support is available with the classic load balancer. For more information, see the AWS online help on configuring proxy protocol support for the classic load balancer.

Many standard load-balancing applications, such as HAProxy, NGINX, or F5 (requires iRules) support proxy protocol. Set the proxy protocol for External S-TAP as follows:

- From the External S-TAP UI , set Proxy Protocol to 1 - Enabled in the External S-TAP group tab.
- From the `container_mgmt.sh` script, specify `--proxy-protocol 1`.
- If you deploy External S-TAP with helm, set `estap.proxy.proxy_protocol` to 1 in the overrides yaml file.
- If you deploy External S-TAP by using Cloud Pak for Data 3.x, set Proxy protocol expected to 1 in the Database and Proxy tab.

Connection to GIM Server fails

External S-TAP does not use GIM. You can ignore all error messages that are related to GIM.

Adding users for PostgreSQL 14 and later

Channel binding is enabled by default for PostgreSQL 14 and later. If your site records passwords with Salted Challenge Response Authentication Mechanism (SCRAM), then the server also supports channel binding. To use External S-TAP when channel binding is enabled, set password encryption when you add new users, as follows:

```
set password_encryption = 'md5'; alter user "username" with password 'newPassword';
```

Connections resetting with AWS Elastic Load Balancer

In general, you can use AWS network load balancing with External S-TAP (as recommended by AWS). However, if you have issues with resetting the connections, then use the classic elastic load balancer (ELB) that allows you to change the idle session timeout.

For AWS ELB, set the idle session timeout to 4000 seconds.

AWS ELB health check generates misleading connections

By default, the AWS ELB health check uses an available traffic port to connect to the database. These connections can be misinterpreted as suspicious activities. To prevent AWS ELB health check from connecting to the database, set the AWS ELB health check port to 22.

Deploying External S-TAP with AWS fails

To deploy External S-TAP with AWS, IAM user must have installed the following AWS EKS policies:

- AmazonEKSClusterPolicy
- AmzonEKSWorkerNodePolicy
- AdministratorAccess
- AmzonEKSServicePolicy
- AmzonEKS_CNI_Policy

Using External S-TAP with a single host

If you use External S-TAP on a Kubernetes cluster that has a single node (which can be the database), then you do not need a load balancing service. Instead of a load balancer, create a **NodePort** service and set the database connection to use the node hostname and **NodePort** for monitoring.

12.1 and later External S-TAP does not support sending early session resumption data

Certain databases such as Elasticsearch and CockroachDB can send session resumption data early during the Transport Layer Security (TLS) handshake instead of sending it after the TLS handshake is complete. External S-TAP currently does not support sending session resumption data early in the process so it cannot forward the session resumption data to the client. Due to this limitation, the UI displays an error and the session gets disconnected.

Related concepts

- [Certificate CLI commands](#)

Guardium Installation Manager

You can use the Guardium® Installation manager (GIM) to install and maintain Guardium components on managed servers.

The GIM component includes a GIM server, which is installed as part of the Guardium system, and a GIM client, which must be installed on servers that host databases or file systems that you want to monitor. The GIM client is a set of Perl scripts that run on each managed server. After you install the GIM client, it works with the GIM server to perform these tasks:

- Check for updates to installed software
- Transfer and install new software
- Uninstall software
- Update software parameters
- Monitor and stop processes that run on the database server

For example, you can use GIM to install your S-TAP modules and keep them up-to-date.

The GIM client uses port 8444 to communicate with the GIM server.

You can use the GIM server through the Guardium user interface or through the command-line interface (CLI).

The software modules that you can deploy by using GIM are packaged as GIM bundles. A *bundle* is a file of type `gim` that contains software that can be deployed by using GIM.

If your environment includes a Guardium system that is configured as a central manager, you must decide which Guardium systems you want to use as GIM servers. You can either manage all of your GIM clients, up to 4000, from a single Guardium system, such as the central manager, or you can manage them in groups from the different Guardium systems. If you manage all of your GIM clients from a single Guardium system, then you can view the status of all the GIM clients and perform related tasks from that one UI. If you choose to manage your GIM clients in groups from separate Guardium systems, then you can use each UI to work with the GIM clients that it manages; no overall view is available. You can view each GIM client only from the Guardium system that functions as its GIM server.

To manage large numbers of GIM installations, you can create groups of GIM clients. Then, you can use the groups to install, update, and manage software bundles.

The GIM client monitors the processes that you install by using GIM. It checks the heartbeat of each process once each minute, and passes status changes for the processes to the GIM server. The status of each process is displayed on the Process Monitoring panel. Changes are reflected within three minutes. Changes to the status of the GIM client itself are reflected according to the interval at which the client polls the server and delivers its "alive message".

Note: When performing a system backup and restore from one server, which has GIM defined, to another server, then the user must configure a GIM failover to the restore server. This GIM configuration applies to a Backup Central Manager or a System backup and restore.

- [**GIM management**](#)
Learn how to manage GIM certificates, run GIM diagnostics and server log, and learn about the GIM failover mechanism.
- [**GIM server allocation**](#)
Remotely connect to a preinstalled and inactive (not connected to any collector) GIM agent and make it connect to some collector without the need to access the database server.
- [**Install, upgrade, and uninstall GIM clients on Linux-UNIX servers**](#)
- [**Install, upgrade, and uninstall GIM clients on Windows servers**](#)
- [**Managing GIM clients**](#)
Learn how to configure the GIM global parameters, how to simplify some GIM tasks by using groups of GIM clients, and learn about GIM dynamic updating.
- [**Managing software with GIM**](#)
- [**Starting and restarting GIM services and components**](#)

GIM management

Learn how to manage GIM certificates, run GIM diagnostics and server log, and learn about the GIM failover mechanism.

- [**Creating and managing custom GIM certificates**](#)
You can replace the default Guardium, privately signed, certificates with trusted CA certificates, without interrupting the GIM server to GIM client communication.
- [**Replacing default GIM certificate with SHA1 or SHA256 certificate**](#)
You can replace the default SHA2 GIM certificates with SHA1 or SHA256 without interrupting the GIM server to GIM client communication.
- [**GIM server failover**](#)
You can define a backup GIM server. If a GIM client fails to connect to its GIM server after five consecutive attempts, the GIM client automatically connects to the failover server if it is specified.
- [**Running GIM diagnostics**](#)
You can run diagnostics on GIM clients to verify that the GIM server has accurate data about each client.
- [**Enable/disable the GIM server log**](#)
You can enable the GIM server log to assist with troubleshooting.

Creating and managing custom GIM certificates

You can replace the default Guardium®, privately signed, certificates with trusted CA certificates, without interrupting the GIM server to GIM client communication.

Before you begin

- All GIM clients must be running v11.0 or higher.

CAUTION:

Failure to upgrade the clients before you start this procedure complicates the certificate distribution process and can require substantial efforts to recover the GIM clients running earlier versions.

- Make sure that a GIM client is registered to the Guardium appliance.
- In adherence to the mutual Transport Layer Security (mTLS) mandate for Guardium Installation Manager (GIM) client-server communication, custom certificates must comply with the following best practices:
 - To ensure streamlined verification processes, certificates must not contain Subject Alternative Name (SAN) entries.
 - If Extended Key Usage (EKU) is used within the certificates, it is essential that they possess both serverAuth and clientAuth properties. This ensures comprehensive authentication capabilities for both server and client endpoints.

About this task

The GIM server-GIM client communication is secured by an encrypted channel and authentication. When you install GIM, it uses default Guardium certificates that are privately signed. Best practice is to install your own certificates from a trusted CA. In both cases, certificates are stored on the GIM server, and distributed to the GIM clients.

When you enable this feature, each GIM client downloads its new certificate, but continues to communicate with the GIM server by using its current certificate. After the new certificates are downloaded to all of the GIM clients, you then install a new certificate on the GIM server, and each GIM client starts by using the new certificate. The clients and their server do not lose any communication.

You can activate GIM listeners after the GIM certificates on the appliance has been changed. See [What to do next](#).

You can observe progress in the GIM Distributed Certificates report, and view GIM events in the GIM Events List report.

The pre-V11.0 method of deploying certificates is fully compatibility with this new method. If you want to deploy certificates by using your own applications, you can configure GIM to use these certificates by using the common GIM update parameters mechanism.

For authentication to succeed, all certificates must be signed by the same CA certificates (root, and intermediate if applicable), whether they are trusted or private.

Certificates expire at some point. Use the command **show certificate warn_expired** to view all expired certificates or certificates that expire within the next six months. When your certificates expire, perform this procedure again with the new certificates.

Procedure

1. Enable the GIM certificate distribution feature. On the central manager, in the GIM Global Parameter page, enter the GIM command:
gim_auto_certificate_distribution=1.
2. Open the Guardium GUI, and in your Dashboard, add the GIM Distributed Certificates Report so you can view progress.
3. Create GIM client certificates. If the Root CA did not change, you do not need to create a server certificate at all. If you are changing the Root CA, you need to create a server certificate, in steps [3.g](#), and [3.h](#).
 - a. Log in to Guardium CLI as CLI user.
 - b. Run **create csr gim client** to create a new CSR with the alias gim. Complete the details:
 - Common Name
 - Organizational Unit
 - Organization
 - City or Locality
 - State or Province
 - Two-letter country code
 - Encryption algorithm (Default: RSA)
 - Keysize (Default: 2048)
 - Subject Alternative Name (Optional)
 - c. Get the CSR signed by either a private CA or trusted CA. The Certificate needs to be in PEM format so that it can be imported into the Guardium appliance. Intermediate and root certificates must be appended.
 - d. Run **store certificate gim client <type>** to store the GIM client certificate into its own keystore, where <type> represents the mode of import:
 - **console**: Paste the Certificate to the console
 - **external**: Import the Certificate from an external location
 - e. If you entered **console** in [3.d](#), paste the end-entity and trusted CA certificates to the console, forming a trusted chain, then press Ctrl+D
 - f. If you entered **external** in [3.d](#), you are prompted to provide the location of where the certificate is stored, and possibly a password.
4. Check the GIM client status by one of:
 - a. Run the CLI command: **show certificate gim client console**. Verify that all intermediate (if applicable) and root certificates are concatenated.
 - b. Look at the GIM client states in the GIM Distributed Certificates report. They should change from Pending to Processing to one of:
 - If the root CA changed: Deployed. New certificates were downloaded but not actively used. The GIM client still uses its original certificates.
 - If the root CA was not changed: Deployed, then Active. New certificates were downloaded and are in use.
- If you're using a new CA for the new certificates, the GIM clients should be in the state Deployed. If you're using a new CA, continue with [5.e](#).
- If you're not using a new CA for the new certificates, the GIM clients should be in the state Active. If you're not using a new CA, continue with [5.f](#).
- If a GIM client remains in the state Processing (or N_A) after the alive cycle passes, the GIM client is either inactive or it cannot process its certificate. Contact Customer support.
5. If you're using a new CA for the new certificates, verify in the GIM Distributed Certificates report that all the client certificates are in the Deployed state.
6. If you're using a new CA for the new certificates, on the primary central manager, create and load the new GIM server certificate.
 - a. Run **create csr gim server** to create a new csr with the alias gim for the gim server certificate.
 - b. Get the GIM server CSR signed by the same CA certificate as used in step [3.c](#).
 - c. Run **store certificate keystore trusted console** to import the trusted CA certificates into the keystore.
 - d. Run **store certificate gim server console** to store the gim server certificate into the keystore. (You can also use the command **store certificate gim server external**. See step [3.f](#).
- Do not change the GIM server certification on the backup central manager.
7. Verify that the GIM Distributed Certificates report that all clients have the state 'ACTIVE' (meaning the clients are connected to the server by using new certificates). It can take up to one complete alive cycle before all clients are in their updated states.
8. If you're using a new CA for the new certificates, update the backup central manager with the new GIM server certificate.
 - a. Log in to the backup central manager.
 - b. Run **store certificate keystore trusted console** to trust and store the CA certificate that was used to sign the gim server certificate.

- c. Run **store certificate gim server console** to store the gim server certificate into the keystore. The root and intermediary certificates (if applicable) also need to be concatenated.
9. Verify in the GIM Distributed Certificates report that all the clients are in the Active state, whether you're using a new CA for the new certificates, or the original CA.

What to do next

You can add GIM clients after you replace the default GIM server certificate. The new GIM clients automatically retrieve the custom certificates in listener mode. Install the GIM client without specifying a collector's IP address (sqlguardip) to ensure it is in listener mode. Then activate the GIM clients. For more information, see [GIM remote activation](#). The certificates are streamed during activation. You can also check that the activated GIM client is listed in the GIM Clients report.

Related concepts

- [Certificate CLI commands](#)

Related tasks

- [Creating dashboards and adding reports](#)

Replacing default GIM certificate with SHA1 or SHA256 certificate

You can replace the default SHA2 GIM certificates with SHA1 or SHA256 without interrupting the GIM server to GIM client communication.

About this task

The GIM server-GIM client communication is secured by an encrypted channel and authentication. When you install GIM, it uses default Guardium certificates that are privately signed. If the GIM client communication fails with the certificate that is installed by default, then you can replace GIM certificates with SHA1 or SHA256. The clients and the server do not lose any communication.

The following conditions must be met for the replace certificate command to work as expected:

- GIM uses default certificates that are privately signed.
- You are using the latest GIM bundle.
- You updated GIM and GIM CA certificates in Tomcat keystore to SHA1 or SHA256.

Procedure

1. To check the currently installed certificate, run the following command on the Guardium CLI.

show certificate gim server

You can see the details of the currently installed certificate.

2. To update the certificate to SHA1 or SHA256, run the following command and enter **y**.

replace certificate gim algorithm

USAGE:**replace certificate gim algorithm < default | default_sha1 >**, where 'default' represents SHA256 and 'default_sha1' represents SHA1 signature algorithm.

3. Restart the Guardium GUI after replacing the default certificate by using the following command.

restart gui

Related concepts

- [Certificate CLI commands](#)

Related tasks

- [Creating dashboards and adding reports](#)
- [Creating and managing custom GIM certificates](#)

GIM server failover

You can define a backup GIM server. If a GIM client fails to connect to its GIM server after five consecutive attempts, the GIM client automatically connects to the failover server if it is specified.

When you install the GIM client, you specify the collector that GIM reports by using the GIM parameter GIM_URL. You can specify another collector for GIM client to fail over to in case primary collector goes down, with the GIM parameter GIM_FAILOVER_URL.

The GIM client reverts to its original GIM server when that server becomes available.

You can add the failover GIM server at any time by using the GIM parameter GIM_FAILOVER_URL.

The GIM server failover has no relationship to the central manager redundancy. The GIM parameter GIM_FAILOVER_URL is not copied or maintained in the backup central manager, so upon central manager switchover there is no defined GIM server.

Running GIM diagnostics

You can run diagnostics on GIM clients to verify that the GIM server has accurate data about each client.

About this task

If you experience trouble with a GIM client, your first step should be to verify that the GIM server has accurate data about that client. Running GIM diagnostics verifies that the modules listed for that client on the GIM server match the modules installed on that client, and that the parameters stored on the GIM client match those stored on the GIM server.

You can run GIM diagnostics either from the Guardium user interface or from the command line. To run from the command line, use this command:

```
grdapi gim_set_diagnostics clientIP=xx.xx.xx.xx
```

The value of clientIP can be either an IP address or a hostname. You must run the command on the Guardium® system that is the GIM server for this client. To run GIM diagnostics from the GUI, use this procedure:

Procedure

1. Use the check boxes next to each client to choose the clients for which you want to run GIM diagnostics.
2. Click Run diagnostics.

The next time that each client polls the GIM server for updates, it will receive the diagnostic command and run it immediately.

Results

You can review the results in the GIM_EVENTS report.

Enable/disable the GIM server log

You can enable the GIM server log to assist with troubleshooting.

Procedure

1. Log in to the CLI of the Guardium® system that the GIM clients point to.
2. Enable debug with the CLI command: **support store debug on GIM**
3. When you have gathered enough details, disable debug with the CLI command: **support store debug off GIM**

Results

The GIM server log is located on the appliance in: /opt/IBM/Guardium/log/gimserver.log

GIM server allocation

Remotely connect to a preinstalled and inactive (not connected to any collector) GIM agent and make it connect to some collector without the need to access the database server.

Overview

Use the following process (also called GIM auto-discovery) to remotely connect to a preinstalled and inactive GIM agent and make it connect to a collector without accessing the database server.

1. An inactive GIM client runs in listener mode and waits for a connection from any collector.
2. From the collector's graphic user interface (GUI) or the GuardAPI, you can send the IP address of any collector to the inactive GIM client.
3. The inactive GIM client accepts the collector's IP address and connects to it.

If GIM is installed without specifying a collector's IP address (--sqlguardip), it runs in listener mode. When the GIM agent is running in server mode, it accepts messages only from verified collectors over SSL that have certificate authentication and shared secret verification. After 30 (or more) consecutive authentication failures, the GIM agent stops listening for requests and runs in server mode. This action prevents denial of service (DoS) attacks.

You can define your own certificates, shared secret, and port number. To use other certificates, specify the certificate/key full path name in the installation parameters: --key_file and --cert_file. See also [Creating and managing custom GIM certificates](#).

To set a shared secret other than the default one, use the GuardAPI command **grdapi gim_set_global_param paramName=gim_listener_default_shared_secret paramValue=<password>**. The shared secret must be identical on the database server and collector.

Note: Do not specify the unencrypted shared secret in the command line.

To use a port other than the default one, specify the port in the installation parameter --listener_port. Set the GIM global parameter **gim_listener_default_port** with the new port in the GIM Global Parameters.

Note: The default or user-defined port must be enabled in the firewall.

Parameters

The following list describes the GIM installation parameters:

- `--sqlguardip` - Sets the collector IP address/hostname that the GIM client is connecting to. If it is not specified, the GIM client runs in "Listener mode".
- `--ca_file` - Full file name path to the certificate authority PEM file.
- `--key_file` - Full file name path to the private key PEM file.
- `--cert_file` - Full file name path to the certificate PEM file.
- `--shared_secret` - specify a shared secret to verify collectors.
- `--listener_port` - specify a port number that is different than the default.
- `--no_listener` - disables GIM from running in "Listener mode" even if `--sqlguardip` is not specified.

Taking any of the following actions causes the GIM agent to exit server mode and process the request.

- Update parameters
- Install modules
- Uninstall GIM directly on the database server

If the GIM client cannot connect to the designated collector, it returns to server mode. After the GIM agent is assigned to a valid collector's IP address or hostname, you cannot set the GIM server to run in server mode again. All new GIM agent server mode parameters appear as READ-ONLY.

Note: The following parameters must exist in the file system or the installation fails:

- `ca_file`
- `key_file`
- `cert_file`

Additional command-line parameter

GIM and Consolidated Installers for GIM have an additional command-line parameter:

`--allow_ip_hostname_combo <0|1>`

This command-line parameter sets the `GIM_ALLOW_IP_HOST_COMBO` GIM parameter. Enter `0` (the default) to disable, and `1` to enable.

When `--allow_ip_hostname_combo <0|1>` is enabled,

- If `GIM_CLIENT_IP` is different than the db server's hostname, `GIM_CLIENTS.GIM_CLIENT_NAME` is set to `hostname_<GIM_CLIENT_IP>`
- If `GIM_CLIENT_IP` is an IP address, the GIM hostname is set to `<hostname>_<GIM_CLIENT_IP>` This naming convention allows GIM clients to be unique across database servers with a common hostname.
- Restriction: You cannot set `GIM_CLIENT_IP` with a common hostname. Using a common hostname is considered as an attempt to register with a duplicate identifier.

Setting GIM in server mode global parameters

You can set up the server mode GIM parameters by using the following GuardAPI command:

```
grdapi gim_set_global_param  
paramName=gim_listener_default_shared_secret  
paramValue=<password>
```

This value is encrypted and stored in the database. The value must be identical to the unencrypted value as the shared secret if you install the GIM agent on the database server.

To set up a new default server mode GIM port, use the following GuardAPI command:

```
grdapi gim_set_global_param paramName=gim_listener_default_port paramValue=<port number>
```

This value must be identical to the unencrypted value of the shared secret if you install the GIM agent on the database server.

Note: If you use a different port or shared secret, you must specify the shared secret or port every time you connect the collector IP/hostname to the server mode GIM agent.

GIM remote activation

Use GIM remote activation to remotely connect to a preinstalled GIM agent and connect it to a collector without accessing the database server. To use GIM remote activation, browse to `Manage > Module Installation > GIM Remote Activation`.

Enter the following information:

1. Host name or IP address or Server group - You can either:
 - Enter the database IP address or host name where GIM is running in listener mode.
 - To activate a group of GIM clients in listener mode, select a server group from the list.Note: If the collector can use either IPv4 or IPv6 addresses, but this appliance supports IPv6 only, enter the IPv6 IP address to prevent errors.
2. GIM Listener Port - Enter the port number if it is different than the GIM Global setting. The default is `8445`.
3. GIM Listener Password - Enter the shared secret if it is different than the GIM Global setting.
4. Guardium hostname or IP address - Specify the hostname or IP address of the Guardium appliance where you want the GIM client to connect. If you leave this field blank, the GIM client connects to the Guardium appliance from which it was activated.
5. Click Submit to save your changes or Reset to exit without saving.

Note: You must either enter an IP address or hostname or select a server group, but the GIM listener port and GIM listener password (shared secret) are optional. When you install the GIM client in listener mode, you cannot change the settings of the shared secret and certificates unless you reinstall the GIM client.

Creating a GIM auto-discovery process

Create a GIM auto-discovery process to identify and associate GIM clients that are installed in listener mode. You can also activate GIM clients that are installed in listener mode by using [Deploy monitoring agents](#).

1. Navigate to Discover > Database Discovery > GIM Auto-discovery Configuration.
 2. Create a GIM auto-discovery process by clicking the  icon.
 3. In Process name, provide a name for the process and then click Apply.
 4. Define hosts to scan for GIM clients that were installed in listener mode using the Add hosts and ports to process section.
 - a. Identify a host or subnet to scan in Host(s). Wildcard characters are allowed. For example, to select all addresses that begin with 192.168.2, use **192.168.2.***.
 - b. To add the host or subnet to the GIM auto-discovery process, click Add scan.
 - c. Repeat the previous steps to define multiple hosts or subnets to include in the GIM auto-discovery process.
- Note:
- If you have a dual stack configuration, define scans for both the IPV4 and the IPV6 addresses.
 - Modify existing host or subnet scans by typing over the existing value and clicking Apply to save the changes.
 - Remove scans by clicking the  icon. If a task has scan results dependent upon it, the scan cannot be deleted.
5. Run the GIM auto-discovery process by clicking Run Once Now or define a schedule for running the process by clicking Modify Schedule. For more information, see [Scheduling](#).
 6. After the process has completed, click View Results to see a list of discovered GIM clients and associate those clients with Guardium systems.
 - a. Select the GIM clients to associate.
 - b. Click Associate to assign the clients to the current Guardium system or click Assign Collector to assign the clients to another Guardium system in your environment.
 - c. Use the Results dialog to review the status of client association. After you associate the GIM clients, the clients are no longer in listener mode and are not shown in the GIM Auto-Discovery Results Viewer window.
 - d. Click Close to close the results window.

GIM global parameters

Define your own shared secret or GIM listener port through the user interface.

1. To open the GIM Global Parameters, click Manage > Module Installation > GIM Global Parameters.
2. Select `gim_listener_default_shared_secret` to set the shared secret or `gim_listener_default_port` to set the port.
3. Click the  icon to edit the selected parameter.
4. Change the value and click Save to change the parameter or Close to return to the page.

Install, upgrade, and uninstall GIM clients on Linux-UNIX servers

Follow best practices when installing or upgrading GIM clients:

- Upgrade to the latest GIM client after upgrading the Guardium system.
- Replace the default GIM certificates with more secure custom certificates. For more information, see [Creating and managing custom GIM certificates](#).

Attention: Read the following information before installing Guardium 12.0 or later: [Updating Guardium Data Protection GIM clients with SHA256 certificates](#)

- [Installing the GIM client on a UNIX server](#)
Learn how to install the GIM client on Unix database servers.
- [Upgrading the GIM client](#)
You can use GIM to upgrade the GIM client to a newer version.
- [Uninstalling GIM and its modules on a UNIX database](#)
You can uninstall GIM and its modules either from the GUI, or on the database server itself.
- [Installing GIM and other packages on Linux servers by using the consolidated installer](#)
Use the consolidated installer to install the GIM client and other agents, such as the S-TAP, CAS, and FAM, on the database server, in a one-step process.
- [Managing GIM clients during a major upgrade of the database server operating system](#)
When you upgrade the operating system on your database server, use the GIM client to automatically upgrade itself and the GIM bundles (for example, GIM, S-TAP, CAS) installed on the Linux-UNIX database. However, most operating systems do not support a major upgrade, for example from RHEL7 to RHEL8.

Installing the GIM client on a UNIX server

Learn how to install the GIM client on Unix database servers.

Before you begin

Disk Space requirements

- Perl 5.8 (and up)
- 1GB of space to accommodate all GIM modules (including maintaining a copy of the previous and current installed versions). Without FAM, 300MB.

Port requirements

- **8445:** GIM client listener, both directions. Any GIM server on either the central manager or the collector can communicate with the GIM client.
- **8443:** (discovery) on the DB server to allow communication from the DB server to the Guardium appliance, and for uploading features.
- **8446:** Used between the GIM client and the GIM server (on the central manager or collector) for authenticated TLS, both directions, custom kernel upload, MustGather loggers upload. If `GIM_USE_SSL` is enabled (default), then the GIM client attempts to communicate its certificate by using port 8446. If port 8446 is not open, then it defaults to 8444, but no certificate is passed (for example, TLS without verification).

- 8081:** Used between the GIM client and the GIM server (on the central manager or collector) for non-TLS (but with message signing verification), both directions, custom kernel upload, MustGather loggers upload. In this scenario, the parameter GIM_USE_SSL must be disabled (=0).

About this task

You can install and use the GIM client in a Solaris slave zone or an AIX workload partition (WPAR). This enables you to use the GIM client to install an S-TAP in a slave zone or WPAR. When you install an S-TAP in a slave zone or WPAR, the K-TAP is disabled, regardless of the setting of the ktap_enabled parameter. You can also use the GIM client to install the Configuration Auditing System (CAS) agent in a slave zone or WPAR. You cannot install the discovery bundle in a slave zone or WPAR; the discovery agent running on the global zone can collect information from other zones. The process for installing the GIM client in a Solaris slave zone or an AIX workload partition is the same as the process for installing in the master zone. The installation can take a few seconds longer than installing in the master zone. If you install the GIM client on a Solaris system with master and slave zones, you must install the client in the same location on the master and slave zones. This location cannot be a shared directory. On Solaris, the GIM client and supervisor in each slave zone are controlled by the GIM supervisor process that runs in the master zone. If the supervisor process on the master zone is shut down, all GIM processes on the slave zones are shut down as well.

Table 1. Installation parameters

| Parameter | Description |
|--------------------------|---|
| dir | Target directory of the GIM client installation. |
| tapip | The IP address or FQDN of the database server or node on which the GIM client is being installed. |
| sqlguardip | The collector IP address/hostname that the GIM client connects to. If it is not specified, the GIM client installs in "Listener mode". |
| no_ssl | Use SSL to encrypt traffic between the GIM client and the Guardium appliance. <ul style="list-style-type: none"> 0: no 1: Use SSL to encrypt traffic between the agent and the Guardium system. This adds ~15% of CPU usage to the GIM client. Guardium® recommends encrypting network traffic between the GIM client and the collector whenever possible: only in cases where the performance is a higher priority than security should this be disabled. |
| perl | Path to perl script, for example: /usr/bin/ |
| ca_file | Full file name path to the Certificate Authority PEM file. |
| key_file | Full file name path to the private key PEM file. |
| cert_file | Full file name path to the certificate PEM file. |
| listener_port | Listener port for registration with appliance. Default = 8445. |
| shared_secret | Set the shared secret to verify collectors. |
| no_listener | Disables "Listener mode" even if sqlguardip is not specified. |
| install_customed_bundles | Allow GIM clients to install custom bundles. <ul style="list-style-type: none"> 0: no 1: yes |
| failover_sqlguardip | The IP address/hostname of the secondary collector with which this GIM client communicates. |
| allow_ip_hostname_combo | Enables GIM client uniqueness across database servers with "common" hostname. <ul style="list-style-type: none"> 0: no 1: yes <ul style="list-style-type: none"> If GIM_CLIENT_IP is an IP address, the GIM client hostname is a combination of the <hostname>_<GIM_CLIENT_IP>. If GIM_CLIENT_IP is set with an IP address and the GIM_ALLOW_IP_HOST_COMBO is enabled, GIM's hostname is a combination of the <hostname>_<GIM_CLIENT_IP>. This allows GIM clients uniqueness across database servers with "common" hostname. You can NOT set GIM_CLIENT_IP with a "common" hostname. This is considered as an attempt to register with a duplicate identifier. |
| auto_set_gim_tapip | When value set to 1, a local IP is automatically assigned. Do not specify both auto_set_gim_tapip and tapip when installing the GIM client. <ul style="list-style-type: none"> 0: no 1: yes Default value is 0. |

Note: Install the GIM client first on the master zone, then on the local.

Procedure

- Place the GIM client installer on the database server in any folder.
- Run the installer: `./installer_name` [-- --dir <install_dir> <--sqlguardip> <g-machine ip> --tapip <db server ip address> --perl <perl dir> -q]

The installer name has the syntax: guard-bundle-GIM-<release build>-<DB>-<OS>_<bit>.gim.sh, for example:

```
guard-bundle-GIM-10.5.0_r103224_v10_5_1-rhel-6-linux-x86_64.gim.sh
```

Attention:

- Omit the --sqlguardip parameter to install the client in GIM listener mode. Listener mode makes the GIM client available for remote registration from a Guardium system. For more information, see [GIM remote activation](#) and [Creating a GIM auto-discovery process](#).
- When cloning database servers and establishing large deployments, use --auto_set_gim_tapip to allocate a random IP address from one of the valid IP addresses of a database server. Do not specify both auto_set_gim_tapip and tapip when installing the GIM client. Update the GIM_AUTO_SET_CLIENT_IP parameter after GIM client installation by using [Manage Module Installation](#). Set up by Client.

- On Red Hat Linux, version 6 or later, run these commands to verify that the files have been added:

```
ls -la /etc/init/gim*
ls -la /etc/gsvr*
```

On Solaris, version 10 or later, run this command:

```
ls /lib/svc/method/guard_g*
```

On all other platforms, run these commands to verify that the following new entries were added to /etc/inittab:

```
gim:2345:respawn:<perl dir>/perl <modules install dir>/GIM/<ver>/gim_client.pl  
gsvr:2345:respawn:<modules install dir>/perl <modules install dir>/SUPERVISOR/<ver>/guard_supervisor
```

Where modules install dir is the directory where all GIM modules are installed, for example, /usr/local/guardium/modules.

4. Enter this command to verify that the GIM client, SUPERVISOR process, and modules are running:

```
ps -afe | grep modules
```

5. Log in to the Guardium system and check the Process Monitoring status.

Upgrading the GIM client

You can use GIM to upgrade the GIM client to a newer version.

Procedure

1. Upload the latest available BUNDLE-GIM.gim file to the Guardium® system.
2. Use the GIM GUI to schedule the installation of the new BUNDLE-GIM.gim file.
3. Monitor the installation process. Click the icon and then click Refresh. When the installation successfully completes the status displays as INSTALLED.

Uninstalling GIM and its modules on a UNIX database

You can uninstall GIM and its modules either from the GUI, or on the database server itself.

Procedure

1. To uninstall using the Guardium GUI.
 - a. Schedule an uninstall of the S-TAP bundle (Setup by Client).
 - b. Schedule an uninstall of the GIM bundle (Setup by Client).
 - c. Reboot the database server to remove K-TAP from the drivers.
2. Alternatively, uninstall on the DB server itself:
 - a. Uninstall both the GIM bundle and the S-TAP bundle by executing as root: **/full/path/modules/GIM/current/uninstall.pl**
 - b. Reboot the database server to remove K-TAP from the drivers.

Installing GIM and other packages on Linux servers by using the consolidated installer

Use the consolidated installer to install the GIM client and other agents, such as the S-TAP, CAS, and FAM, on the database server, in a one-step process.

Before you begin

Download both the GIM and S-TAP installation packages from [Fix Central](#), and optionally CAS and FAM bundles.

About this task

The consolidated installer is supported on:

- AIX, Solaris, Linux (Red Hat, Linux for System z)
- Guardium central managers
- Guardium stand-alone systems

Procedure

1. Use root access and create a directory on the database server.
2. Copy the shell installers for GIM bundles (for example, BUNDLE_GIM, BUNDLE_STAP, BUNDLE_CAS, BUNDLE_FAM) to the new directory.
3. Copy the script consolidated_installer.sh to the same directory and make sure that this script has the execute permission. (If not, then change it.)
4. Run the script.

```
./consolidated_installer.sh --installdir <install dir> --tapip <ip or hostname> --gim_sqlguardip <ip or hostname> --perl <perl dir> [--no_ssl] [--install_customed_bundles] [--failover_sqlguardip <ip or hostname>] [--allow_ip_hostname_combo <0|1>] [-auto_set_gim_tapip]
```
5. To also install BUNDLE_STAP, add the following parameters: --stap_sqlguardip <ip or hostname> [--load-balancer-ip <load_balancer_ip> --lb-app-group <app_group> --lb-mu-group <mu_group> --lb-num-mus <number_of_mus> --ktap_allow_module_combos --use_discovery <0|1> --privatetapip <tapip>]
6. To also install BUNDLE_CAS, add the following parameters: [--cas_sqlguardip <ip or hostname>] --javadir <java directory, excluding the /bin/java from the path>
7. To also install BUNDLE_FAM, add the following parameters: [--icm_url <icm url>] [--fam_port <fam port>] --fam_source_directories <comma delimited directories.no spaces allowed>
8. After the installation is complete with a successful message, check that the modules are installed on the database server, and that they are running. For example,

- ps -eaf | grep gim: to check the GIM module
 - ps -eaf | grep modules: to check the all modules
9. Verify that the modules are running. Go to Reports > Guardium Operational Reports > GIM Installed Modules, and verify that the modules are installed.
10. Go to Reports > Real-Time Guardium Operational Reports > GIM Events List, and verify status for each GIM bundle installation.

Results

First GIM is installed. GIM looks in the deploy folder for the files, and then installs the other packages, all in the /deploy directory. The S-TAP with all of its components is installed under the guardium installation directory along with the GIM.

Related concepts

- [Linux-UNIX: S-TAP install script parameters](#)
- [File discovery and classification GIM parameters](#)
- [Prerequisites, installing and running CAS on a Linux-UNIX server](#)
- [Installing CAS from the CLI on a Windows server](#)
- [Windows: Monitoring with the Guardium Agent Monitor](#)

Related reference

- [Linux-UNIX: S-TAP GIM installation parameters](#)
- [Linux-UNIX: S-TAP guard-config-update parameters for RPM installation and update](#)
- [Windows: S-TAP GIM installation parameters](#)
- [Windows: S-TAP command line installation parameters](#)

Managing GIM clients during a major upgrade of the database server operating system

When you upgrade the operating system on your database server, use the GIM client to automatically upgrade itself and the GIM bundles (for example, GIM, S-TAP, CAS) installed on the Linux-UNIX database. However, most operating systems do not support a major upgrade, for example from RHEL7 to RHEL8.

Before you begin

The target upgrade GIM bundles must be available on the GIM server. The build number of each bundle must be the same or greater than the bundle that is installed. Download from [Fix Central](#).

About this task

This procedure is only relevant for databases whose operating system can be upgraded. If you cannot upgrade the operating system, you must uninstall the S-TAP, install the new operating system, and install the S-TAP bundle that is compatible with the newly installed operating system.

GIM bundles are OSType/OsVersion/Processor specific. When the OS version changes (for example, from RHEL7 to RHEL8), all the bundles need to be upgraded.

The GIM parameter auto_install_on_db_server_os_upgrade controls GIM's ability to auto-upgrade all bundles. If enabled, when the database server boots up after an operating system upgrade, GIM automatically downloads and install these bundles. This parameter is disabled by default, to prevent unintentional bundle upgrades.

If the parameter is disabled when you upgrade the database operating system, the GIM client detects that the operating system changed, and it changes the _x suffix of the version to _0. You can see the version in the Set up by Client, for example, 10.6.1.4_r123456_0. To resolve the mismatch between the GIM client and the database operating system, do one of:

- Enable the GIM global parameter auto_install_on_db_server_os_upgrade, which automatically upgrades all the GIM clients with the latest bundle of the operating system they support.
- Do not enable auto_install_on_db_server_os_upgrade, and upgrade the GIM clients manually.

It is best to update all your GIM-installed modules as soon as possible after the upgrade, whether manually or automatically. K-TAP is not loaded after an operating system upgrade.

Procedure

1. Log in to the CLI of the Guardium system that is the GIM server
2. Enable auto_install_on_db_server_os_upgrade by entering:

```
grdapic gim_set_global_param paramName="auto_install_on_db_server_os_upgrade" paramValue="1"
```

3. Upgrade the operating system on your database server.

Results

At first boot after OS upgrade, the GIM client recognizes that the operating system was upgraded and:

1. Changes the configuration files for all GIM-installed modules to support the new operating system attributes.
2. Registers all the modules to the GIM server with the updated attributes. This change triggers the GIM server to look for a bundle that has the same build number as the previously installed bundle, but is compatible with the upgraded operating system. If it does not find such a bundle, it looks for the latest bundles that

support the new operating system attributes. When the server finds appropriate bundles, it schedules them for upgrade and runs the upgrade process immediately. If the server cannot find appropriate bundles, it issues an error message.

3. Records an alert in the GIM_EVENTS report, that an operating system upgrade occurred and lists the actions that should be taken.

What to do next

Review the messages in the GIM_EVENTS report. If the GIM server reports that the modules were upgraded successfully, verify the proper operation of the modules as you would do after any update.

If error messages were written to the GIM_EVENTS report, indicating that the upgrade was not successful, review the error messages for guidance.

When the operating system upgrade is complete, disable the automatic update option on the GIM server to prevent a GIM client from erroneously starting an update process.

```
grdapi gim_set_global_param paramName="auto_install_on_db_server_os_upgrade" paramValue="0"
```

Install, upgrade, and uninstall GIM clients on Windows servers

Follow best practices when installing or upgrading GIM clients:

- Upgrade to the latest GIM client after upgrading the Guardium system.
- Replace the default GIM certificates with more secure custom certificates. For more information, see [Creating and managing custom GIM certificates](#).

Attention: Read the following information before installing Guardium 12.0 or later: [Updating Guardium Data Protection GIM clients with SHA256 certificates](#)

- [Installing the GIM client on a Windows server](#)

Learn how to install the GIM client for Windows by using either an interactive installer or a silent installation. Instructions are also provided for uninstalling the GIM client.

- [Installing GIM and other packages on Windows servers by using the consolidated installer](#)

Use the consolidated installer to install the GIM client and other agents, such as the S-TAP, on the database server, in a one-step process.

- [Starting and stopping the GIM client on a Windows server](#)

Learn to start and stop the GIM client on a Windows server.

Installing the GIM client on a Windows server

Learn how to install the GIM client for Windows by using either an interactive installer or a silent installation. Instructions are also provided for uninstalling the GIM client.

About this task

The Windows GIM client installer changed to a .NET based installer in v10.1. The installer for the GIM client is based on your GIM client version. Build numbers start from 10.2.30.5.

Port requirements

- **8445:** GIM client listener, both directions. Any GIM server on either the central manager or the collector can communicate with the GIM client.
- **8443:** (discovery) on the DB server to allow communication from the DB server to the Guardium appliance, and for uploading features.
- **8446:** Used between the GIM client and the GIM server (on the central manager or collector) for authenticated TLS, both directions, custom kernel upload, MustGather loggers upload. If GIM_USE_SSL is enabled (default), then the GIM client attempts to communicate its certificate by using port 8446. If port 8446 is not open, then it defaults to 8444, but no certificate is passed (for example, TLS without verification).
- **8081:** Used between the GIM client and the GIM server (on the central manager or collector) for non-TLS (but with message signing verification), both directions, custom kernel upload, MustGather loggers upload. In this scenario, the parameter GIM_USE_SSL must be disabled (=0).

Installing the GIM client with an interactive installer

A wizard is provided to help you install the GIM client on each database server.

About this task

You can specify a custom key, certificate, and CA file when you install the GIM client in both standard mode and in listener mode. For more information, see [Creating and managing custom GIM certificates](#).

Procedure

1. Place the GIM client installer on the database server, in any folder.
2. Run the setup.exe file to start the wizard that installs the GIM client.
The setup.exe file is located in the GIM-Installer-<version> folder.
3. Follow and answer the questions in the installation wizard.

What to do next

You can view the results of the installation in the log file at C:\IBM Windows GIM.ctl.

Installing the GIM client with silent installation

If you prefer, you can install the GIM client from the command prompt instead of the wizard.

Procedure

1. Place the GIM client installer on the database server, in any folder.
2. Open a command prompt and navigate to the GIM_Installer* folder under the folder where you placed the installer.
3. Enter the following command, with no line break:

```
setup.exe -UNATTENDED -INSTALLPATH "c:\Program Files(x86)\Guardium Installation Manager" -LOCALIP <GIM CLIENT IP> -  
APPLIANCE <Appliance IP>
```

Attention:

- The UNATTENDED and LOCALIP parameters are required. APPLIANCE is optional and if not supplied, triggers Listener Mode.
- Do not specify both AUTO_ASSIGN_IP parameter and LOCALIP.
- Omit the APPLIANCE parameter to install the client in GIM listener mode. Listener mode makes the GIM client available for remote registration from a Guardium system. Example of how to install as listener:
`setup.exe -UNATTENDED -INSTALLPATH "c:\Program Files(x86)\Guardium Installation Manager" -LOCALIP <GIM CLIENT IP>`
For more information, see [GIM Remote Activation](#) and [Create a GIM Auto-discovery Process](#).
- When cloning database servers and establishing large deployments, use auto_assign_ip 1 to allocate a random IP address from one of the valid IP addresses of a database server. Do not specify both auto_assign_ip and localip when you install the GIM client. When you update the GIM_AUTO_SET_CLIENT_IP parameter by using `ManageModuleInstallation`. Set up by Client, you must restart the GIM client service for the new setting to take effect.

Table 1. Parameters applicable to all .NET installers

| GIM parameter | Description |
|------------------|---|
| -UNATTENDED | Install silently. A value is not required. |
| -UNINSTALL | Uninstall. A value is not required. |
| -INSTALLPATH | The installation directory. The default installation path is "C:\Program Files (x86)\Guardium\Guardium Installation Manager". |
| -CUSTOMER | Change customer name. |
| -COMPANY | Change company name. |
| -SERVICEUSER | Specify a user to run the service under. |
| -SERVICEPASSWORD | The password for the user. |

Table 2. Parameters specific to GIM .NET installers

| GIM parameter | Description |
|-------------------|---|
| -APPLIANCE | To set the appliance address that GIM connects to. If not specified, GIM installs in Listener Mode. |
| -AUTO_ASSIGN_IP | When the value is set to 1, a local IP is automatically assigned. In this case, do not specify the local IP with -LOCALIP. Default value is 0 (do not auto-assign the IP address). |
| -CA_FILE | Set the CA file to non-default file. |
| -CERT_FILE | Set the certificate file to non-default file. |
| -INSTALLERLOGPATH | Specifies the location for storing the S-TAP installer log files. Use this parameter if you don't want to use the default location (C:). |
| -KEY_FILE | Set the key file to non-default file. |
| -LISTENER_PORT | If you do not use the -APPLIANCE parameter, then set the -LISTENER_PORT for registration with appliance. Default value is 8445. |
| -LOCALIP | The IP of the server where you are installing GIM. |
| -NO_SSL | Use SSL to encrypt traffic between the GIM client and the Guardium appliance. <ul style="list-style-type: none">• 0: Do not use SSL.• 1: Use SSL to encrypt traffic between the agent and the Guardium system. Using SSL adds ~15% of CPU usage to the GIM client. Guardium recommends that you encrypt network traffic between the GIM client and the collector whenever possible. Disable this parameter only when performance is a higher priority than security. |
| -SHARED_SECRET | Set a shared secret for registration with appliance if not specified by using -APPLIANCE parameter. |

What to do next

You can view the results of the installation in the log file at C:\IBM Windows GIM.ctl.

Uninstalling the GIM client

Procedure

1. Open a command prompt and navigate to the GIM_Installer* folder under the folder where you installed the client.
2. Enter the following command:

```
setup.exe -UNINSTALL
```

Installing GIM and other packages on Windows servers by using the consolidated installer

Use the consolidated installer to install the GIM client and other agents, such as the S-TAP, on the database server, in a one-step process.

Before you begin

Download both the GIM and S-TAP installation packages from [Fix Central](#).

About this task

Each agent installer package (WINSTAP, CAS, GAM) has a folder called Gim-Kits that contains a conf.reload.* and a signed file. The conf.reload files have the agent configuration parameters, which are the same as the parameters in the other installation packages. The conf.reload.* files need editing for your specific environment. The signed files do not need editing.

Procedure

1. Copy the GIM installer to the database server.
2. Create a folder called `deploy` in the GIM installer directory.
3. Examine the conf.reload.* files and make any configuration changes for the S-TAPs in your environment. For example, the sqlguard IP setting or the enterprise load balancing settings.
4. Customize the conf.reload.* files for all other packages you are going to install.
5. Copy all of the edited conf.reload files, and the SIGNED files, into the `deploy` folder that you created in step 2.
6. Install the GIM with the CLI, or the wizard on a Windows server. For example:
`setup.exe -UNATTENDED -AUTO_ASSIGN_IP 1 -APPLIANCE <IP>`
where APPLIANCE <IP> is the GIM Server.

Results

First GIM is installed. GIM looks in the `deploy` folder for the files, and then installs the other packages, all in the `/deploy` directory. The S-TAP is installed with all of its components, located under the `guardium` installation directory along with the GIM.

Related concepts

- [Linux-UNIX: S-TAP install script parameters](#)
- [File discovery and classification GIM parameters](#)
- [Prerequisites, installing and running CAS on a Linux-UNIX server](#)
- [Installing CAS from the CLI on a Windows server](#)
- [Windows: Monitoring with the Guardium Agent Monitor](#)

Related reference

- [Linux-UNIX: S-TAP GIM installation parameters](#)
- [Linux-UNIX: S-TAP guard-config-update parameters for RPM installation and update](#)
- [Windows: S-TAP GIM installation parameters](#)
- [Windows: S-TAP command line installation parameters](#)

Starting and stopping the GIM client on a Windows server

Learn to start and stop the GIM client on a Windows server.

Procedure

1. Log on to the database server system using a system administrator account.
2. From the Services control panel, start or stop the IBM Security Guardium Installation Manager.

Managing GIM clients

Learn how to configure the GIM global parameters, how to simplify some GIM tasks by using groups of GIM clients, and learn about GIM dynamic updating.

- [GIM global parameters](#)
Define global parameters for GIM clients using the GIM Global Parameters page or the `gim_set_global_param` API.
- [Using groups with GIM](#)
You can use groups of GIM clients to simplify some GIM tasks.
- [GIM dynamic updating](#)
GIM clients check for updates from the GIM server at regular intervals. The GIM server can calculate the best polling interval to use based on system conditions.

GIM global parameters

Define global parameters for GIM clients using the GIM Global Parameters page or the `gim_set_global_param` API.

Define parameters using the GIM Global Parameters page

1. From the Guardium UI, open `Manage > Module Installation > GIM Global Parameters`.

2. Select a parameter and click the  icon.
3. Use the Global Parameter dialog to edit the selected parameter.
4. Click Save.

Define parameters using the `gim_set_global_param` API

1. From the Guardium CLI, run the API command:

```
grdapi gim_set_global_param paramName=<parameter name> paramValue=<parameter value>
```

Where `<parameter name>` and `<parameter value>` are replaced with parameter name and value being defined.

GIM global parameters

| Parameter name | Value type | Description |
|--|------------|--|
| <code>auto_install_on_db_server_os_upgrade</code> | Boolean | If enabled, automatically upgrade modules when the client operating system vendor version changes. Valid values: <ul style="list-style-type: none"> • 0: Disabled • 1: Enabled Default = 0
For more information, see Linux®-UNIX: Managing GIM clients when upgrading your database server operating system , and Windows: Managing S-TAP when upgrading your database operating system . |
| <code>dynamic_alive_enabled</code> | Boolean | Controls the dynamic alive feature. Valid values: <ul style="list-style-type: none"> • 0: Disabled • 1: Enabled Default = 0
For more information, see GIM dynamic updating . |
| <code>enable_secure_unauthenticated_communication</code> | Boolean | If enabled, allow unauthenticated GIM communication over a secure port: communication between the GIM client and server are encrypted with SSL on port 8444, but the communication is handled without using certificates for peer authentication. Valid values: <ul style="list-style-type: none"> • 0: Disabled • 1: Enabled Default = 0
The <code>enable_secure_unauthenticated_communication</code> allows distributing new GIM client certificates when it is time to replace certificates. |
| <code>gim_auto_certificate_distribution</code> | Boolean | Controls automatic distribution of certificates to GIM clients. Valid values: <ul style="list-style-type: none"> • 0: disabled • 1: enabled Default = 0
For more information, see Create and manage GIM certificates . |
| <code>gim_file_upload_token</code> | string | Define the GIM file upload exchange token. |
| <code>gim_listener_default_port</code> | string | Define the GIM listener default port.
Default = 88445
For more information, see Gim server allocation . |
| <code>gim_listener_default_shared_secret</code> | string | Define the GIM listener encrypted shared secret.
For more information, see Gim server allocation . |
| <code>gim_quick_start_enabled</code> | Boolean | Controls the GIM quick start feature. Valid values: <ul style="list-style-type: none"> • 0: disabled • 1: enabled Default = 0 |

Related reference

- [gim_set_global_param](#)
- [gim_get_global_param](#)

Using groups with GIM

You can use groups of GIM clients to simplify some GIM tasks.

About this task

You can create groups of GIM clients and use them to roll out updates to those managed servers.

Procedure

1. Open the group builder by navigating to Setup > Tools and Views > Group Builder.
2. Click  to open the Create new group dialog.
3. Define the group:
 - Enter a group description.
 - Application type: Public.
 - Group type: Client Hostname.Click Save.
4. To add members by filtering for GIM clients:
 - a. In the Members Tab, click Import and select From query.
 - b. In the Import by query tab, select a report name that begins with GIM, for example, GIM Client Status. The Client hostname drop-down appears.
 - c. In each Enter ... (Like) field, enter a value to be matched, or % to ignore this field when matching clients.
5. To add members individually, in the Members Tab, click , and enter clients by IP or hostname.
6. Click Save.

Results

You can use the group in the Manage > Module Installation > Set up by Client screen to work with this set of clients as a group rather than individually.

GIM dynamic updating

GIM clients check for updates from the GIM server at regular intervals. The GIM server can calculate the best polling interval to use based on system conditions.

Each GIM client sends an "alive" message to its GIM server regularly, to check whether any updates are ready to be processed. This polling interval is calculated and updated based on conditions at the GIM server. The interval is calculated regularly, and the new value is passed to the GIM client in response to its "alive" message. This feature is enabled by default, but you can turn it off if you prefer a fixed interval.

Dynamic updating is controlled by the Guardium API command **gim_set_global_param**, with these parameters.

dynamic_alive_enabled
Dynamic alive feature control. 1 – enabled, 0 – disabled. Default =1
dynamic_alive_check_interval
The interval, in minutes, at which the polling interval is recalculated. Default = 5

For example:

```
grdapic gim_set_global_param dynamic_alive_enabled=0
```

When each GIM client sends its alive message to the server, the server responds with the new polling interval as well as any other updates that have been scheduled for that client.

These parameters were valid in 10.0, and removed from 10.1 and higher:

- **dynamic_alive_default_load_factor**
- **dynamic_alive_cpu_level1_threshold**
- **dynamic_alive_cpu_level2_threshold**
- **dynamic_alive_db_conn_level1_threshold**
- **dynamic_alive_db_conn_level2_threshold**
- **dynamic_alive_cpu_load_sample_time**

Managing software with GIM

- **[Deploy monitoring agents](#)**
Use the Deploy Monitoring Agents tool to automatically activate GIM clients, install S-TAPs, and begin monitoring database traffic.
- **[Set up by Client](#)**
Quickly deploy S-TAPs and other software packages by using the GIM Set up by Client tool.
- **[Uploading and importing GIM modules](#)**
Use the Upload Modules page to upload, import, view, and delete GIM bundles and modules.
- **[Centralized module view](#)**
The Centralized module view is available from any GIM server and lists all bundles and modules present in a Guardium environment.
- **[Managing bundles by using the configurator.sh script](#)**
Use the configurator.sh script to list the installed modules and bundles that are managed by GIM, and to display and change any parameter for the bundles.
- **[GIM CLI commands](#)**
You can use the CLI to install and upgrade modules on the database server.
- **[GIM user interfaces](#)**
The purpose of GIM is to provide automatic installation capability for modules, taking advantage of a GIM client residing on each database server and a GIM server on the Guardium system.
- **[Distributing GIM bundles to managed units](#)**
You can distribute GIM bundles to managed units in order to deploy them on the GIM clients managed by those managed units.
- **[Removing unused GIM bundles](#)**
You can remove GIM bundles from your GIM server if they are no longer used on any database server.

Deploy monitoring agents

Use the Deploy Monitoring Agents tool to automatically activate GIM clients, install S-TAPs, and begin monitoring database traffic.

The deploy monitoring agents tool simplifies the process of establishing a Guardium deployment. Building on existing Guardium installation manager (GIM) infrastructure, the deploy monitoring agents tools helps you quickly find database servers, install monitoring agents (S-TAPs), and configure inspection engines for your databases. In addition, the tool provides a centralized view for tracking and reviewing deployment status.

Prerequisites

Review prerequisites and restrictions before you begin deploying monitoring agents.

Before using the deploy monitoring agents tool to install S-TAPs and configure inspection engines on your database servers, verify the following prerequisites.

The target S-TAP installation directory must be empty or not exist.

You cannot install an S-TAP into a directory that already contains any files.

Review S-TAP prerequisites

[Windows: Prerequisites: Installing S-TAP](#)

[Linux-UNIX: S-TAP installation prerequisites](#)

Install GIM clients in listener mode

Install GIM clients in listener mode on one or more database servers in your environment. To install the GIM client in listener mode on Windows systems, omit the `-host` parameter. To install the GIM client in listener mode on systems such as AIX and Linux, omit the `--sqlguardip` parameter. For more information about GIM listener mode, see [GIM server allocation](#).

Important: You may need to open a port between the GIM client on the database server and the Guardium system where you will run the deploy monitoring agents tool. The default port 8445 is used unless you specify a different port when installing the GIM client.

Upload GIM S-TAP modules to the Guardium system

Run the deploy monitoring agents tool as an administrative user from any Guardium system that is not configured as an aggregator. Before you begin, use the following procedure to upload GIM S-TAP modules to the Guardium system.

1. Navigate to Manage > Module Installation > Upload Modules.
2. Click Choose file and select the module you want to install.
3. Click Upload to upload the module to the Guardium system. After uploading, the module will be listed in the Import uploaded modules table.
4. In the Import uploaded modules table, click the check box next to the module you want to install. The module will be imported and made available for installation. After the module is imported, the Upload Modules page will reload and the module will no longer appear in the Import uploaded modules table.

For information about S-TAP offerings and supported platforms, see [System requirements and supported platforms for IBM Security Guardium](#).

Verify that all discoverable database servers are running

Inspection engines can be automatically configured for some databases, including the following:

- DB2 for Linux, UNIX, and Windows
- Informix
- Microsoft SQL Server
- MySQL
- Oracle
- PostgreSQL
- Sybase
- Teradata

To allow the auto-configuration of inspection engines, verify that databases servers are running before deploying monitoring agents.

For more information about automatically discovering database instances, see [Discover database instances: Windows: Discover database instances](#).

Deploying agents

Learn how to quickly deploy S-TAPs and configure inspection engines for monitoring database traffic.

Before you begin

Run the deploy monitoring agents tool as an administrative user from any Guardium system that is not configured as an aggregator. Verify the following before you begin:

- GIM clients are installed in listener mode.
- GIM S-TAP modules are imported to the Guardium system.
- Discoverable database servers are running.

For more information, see [Prerequisites](#).

Procedure

1. Open the deploy monitoring agents tool by navigating to Setup > Smart Assistant > Deploy Monitoring Agents.

2. In the Identify database servers section, use the IP addresses field to specify a range of IP address to search for GIM clients in listener mode.

Use the  icon to specify additional IP addresses. Include wildcard (*) or range (-) characters to expand the search. For example, 10.0.0-5.*. Use commas to separate complete IP addresses or ranges. For example, 9.70.145.165, 9.70.145-148.165, 9.70.145.*.

Important: Scanning a large number of IP addresses is time intensive and may time-out before the scan completes. Use the IP addresses fields to define a narrow range of IP addresses where you expect to find GIM clients in listener mode.

3. Click Discover to begin scanning for GIM clients in listener mode.

Tip: By default, the discovery of GIM clients and the deployment of monitoring agents (S-TAPs) is completed in two separate steps: discovery, then deployment.

This allows you to manually select the database servers where you want to install S-TAPs, as described in the following steps.

However, it is possible to streamline the process by automatically installing S-TAPs on all compatible GIM clients that are discovered while scanning IP addresses.

To enable the automated mode, click  to open the Customize settings dialog and select Automatically deploy agents on discovered database servers. When using the automated mode, after specifying the IP addresses to scan, simply click the Discover and Deploy button.

- In the Database server status section, select the database servers where you would like to deploy monitoring agents and click Deploy Agents to open the Configure monitoring agents dialog.
- From the Configure monitoring agents dialog, review and adjust the installation parameters. Click Deploy to begin installing monitoring agents. The default parameters should work well for most new deployments. However, you may want to adjust the following settings for your specific environment.

Windows installation directory

Specify an installation directory for S-TAPs deployed on Windows database servers. The parameter is ignored and default installation paths are used when deploying on other platforms. For more information about S-TAP installation parameters, see [S-TAP command line and GIM installation parameters](#) and [S-TAP install script parameters](#).

Assign a Guardium collector

Select Use enterprise load balancing to automatically assign S-TAPs based on the relative load or availability of Guardium collectors in a centrally-managed environment. For more information, see [Enterprise load balancing](#).

Select Specify collector to assign S-TAPs to a specific Guardium collector.

- In the Database server status section, use the S-TAP installation status column to monitor the progress of module installation. A status of **Installed** indicates successful and complete installation.

What to do next

If the S-TAP installation status of a database server is marked **Failed**, click the  icon to learn more about the problem. If a database server disappears from the Database server status after attempting to deploy monitoring agents, click Error log (if a log is available) to learn more about the problem.

Tip: The Error log captures issues related to the Deploy monitoring agents tool. For example, if Deploy monitoring agents cannot find a module required for installation, a message is added to the Error log. Other errors are recorded in component-specific logs and made available for investigation by clicking the  icon in the S-TAP installation status column.

After successfully deploying monitoring agents, you are ready to monitor traffic on your database servers and begin meeting security compliance requirements. To configure compliance monitoring, navigate to [Setup > Smart Assistant > Compliance monitoring](#) and see [Compliance monitoring](#) for more information.

Set up by Client

Quickly deploy S-TAPs and other software packages by using the GIM Set up by Client tool.

Before you begin

Before you use the Set up by Client tool, verify the following items:

- GIM clients are installed on database servers and connected to the Guardium system.
- Compatible GIM bundles are uploaded and imported to the Guardium system.

About this task

The Set up by Client page includes a column named Installed Version. If the version ends with _0, it means that the operating system on the database changed (as part of a system reboot). In this scenario, the GIM client also needs upgrading. In this situation, upload the GIM client bundle that supports the new OS to the Guardium system. Then do one of:

- Enable the GIM Global parameter auto_install_on_db_server_os_upgrade on the Guardium system that is the GIM client, which automatically upgrades all of the GIM clients with the latest bundle of the OS they support.
- Keep auto_install_on_db_server_os_upgrade disabled and do the upgrade yourself,

Procedure

- Go to [Manage > Module Installation > Set up by Client](#).
- In the Choose clients section, select the database servers where you want to install or update software using GIM. Select individual clients using check boxes in the table, or use the Select client group menu to select a group of clients.

Attention:

- To create a client group, click  to open the Create client group dialog. Click Add Clients to open the Existing Clients window, select the clients, and click OK.
- To import clients from a CSV file. Click Import from CSV, and selecting your CSV file. Modify the field delimiter if relevant. Click Load to create a group of type Client Hostname, with Application type of Public. This group can be accessed and managed from the Group Builder.
- After you modify the client list, click  to update the display.
- Use Reset Connection to remove GIM client information from the Guardium system before reregistering the client. After clicking Reset Connection, it might take a few minutes before the status of the GIM client process is reflected.
- Select a client and click View Installed Modules. The View Installed Modules window shows all the modules that are installed on this client (including S-TAP), their versions, and if any module is in pending state for all the selected clients. (The module COMMON, if it appears, can be ignored.)
- When you create or update a group and edit the Client Name of GIM clients, the host name and address must reflect a valid value for a GIM client that is connected to the Guardium system. If an invalid host name is specified, the edited client does not appear as a member of the group. Adding clients by IP address is not supported.

Click Next to continue.

- In the Choose bundle section, use the Select a bundle menu to identify the software you want to install or update. Click Next to continue. After selecting a software bundle, the Selected bundle action column indicates the action that will be performed for each client:

Install

The selected bundle will be installed on the client. This action indicates a first-time installation of the software on the client.

Upgrade

The bundle will be upgraded on the client. This action indicates that an earlier version of the software is currently installed on the client.

Update parameters

The bundle parameters will be updated on the client. This action indicates that the selected software and the currently-installed software are the same version.

None (bundle not found)

No actions will be performed, indicating that there are no compatible actions on the client for the selected bundle.

None (newer version installed)

No actions will be performed because the selected bundle is older than the version that is currently installed on the client. To install an older version of software, first uninstall the current version.

The Available column indicates whether the selected software is available for installation from the GIM server. If the software is not available, click Import Bundles to upload and import the bundle or module.

Tip:

- You can filter the clients, for example, by name, module, Selected bundle actions, and client OS. The resulting selection is persistent; **the action is applied only to the filtered list of clients**. You can see that the number of clients in the Choose Clients section is greater than the number in Configure Clients section.
- Clear the Show only latest versions checkbox to view and work with earlier versions of a bundle.
- Clear the Show only bundles checkbox to identify individual modules within a bundle.
- Select the Show only compatible clients checkbox to hide clients that are not compatible with the selected bundle.

Attention:

- By default, the Select a bundle menu shows only the latest uploaded bundle version regardless of platform or compatibility with selected clients. To install a different bundle version for a specific platform or client, clear the Show only latest versions checkbox and select the required bundle.
- If you upload and import new bundles while working in the Set up by Client tool, refresh the browser to see the new bundles.
- If you have a bundle that is already scheduled for installation, installing a new bundle removes the existing schedule.

4. In the Choose parameters section, specify values for the required and optional parameters. Use the or icons to add or remove optional parameters. Use the icon to search for parameters by name or description. Click Next to continue.

Important: Unless identified as a client-specific parameter, values that are provided in the Choose parameters section are applied to all clients where the software will be installed, upgraded, or updated. For client-specific parameters, the value field is unavailable and values are defined per-client in the Configure clients section.

5. In the Configure clients section, use the table to review, and edit parameter values for each client.

Editable parameters show a icon next to the parameter value. Click the icon to edit the value. The Selected bundle action column shows the action that will be performed on each client.

6. Click Install to begin the software installation. Use the icon to schedule the installation, then click OK to continue.

7. To create the Guardium API syntax for the current configuration in the Setup by Client, click Generate GuardAPI. If enough information is available, it generates API commands for multiple clients in the GuardAPI commands dialog. If there isn't enough information, it shows a default template.

What to do next

In the Success dialog, click Show Status to open the Status window to monitor the software install/upgrade. Click to refresh the results. If an install/upgrade has a failed status, click Uninstall if you see the button, otherwise, click Reset connection.

If you see a Failed installation status for a bundle or module, open the Choose bundle section, select the client, click Uninstall, and use the icon to monitor the installation status. If the Uninstall button is not available, open the Choose clients pane, select the affected client, and click Reset connection. Use the icon to monitor the client list as the connection is reset.

Uploading and importing GIM modules

Use the Upload Modules page to upload, import, view, and delete GIM bundles and modules.

About this task

The Upload module page opens the list of all modules and bundles on the Guardium system, their status (imported or uploaded), their OS and version, and the date they were imported. You can modify the view by:

- Use the free text filter.
- Hide earlier versions of a bundle or module by checking Show only latest version in the table header.
- View the modules included in a bundle. Click next to a bundle name.
- Expand all bundles. Click Expand all modules in the table header.

Procedure

1. Go to Manage > Module Installation > Upload Modules.

2. To upload a module:

- a. Click to open the Upload module dialog.
- b. Click Browse and select a GIM bundle or module to upload.
- c. Click Upload.
- d. In the Confirmation dialog, select one of:
 - Import now: Imports the bundle or module and makes it available for deployment to GIM clients. The resulting status is *Imported*.
 - Import later: Does not import the bundle or module. The resulting status is *Uploaded*.

3. To import one or more bundles or modules, select each one and click Import

4. To delete a bundle or module, select it and click and click Yes to confirm.

Only bundles and modules that are not being used by a GIM client can be deleted. Deleting a bundle or module removes it both from the Upload Module table and from the file system.

Centralized module view

The Centralized module view is available from any GIM server and lists all bundles and modules present in a Guardium environment.

Open the view at Manage > Module Installation > Centralized Module View

Note: Only bundles and modules present on V11.2 and later systems are displayed.

The Centralized module view table supports the following actions:

- The GIM server column shows the total number of servers that have the bundle or module available locally.
- Use the  icon next to a bundle or module to show the specific servers that have it available locally.
- Use the Expand all modules button to expand and view all modules in all bundles.
- Select a bundle and click View modules in bundle to view the modules in the bundle and the servers where they are available.

Managing bundles by using the configurator.sh script

Use the configurator.sh script to list the installed modules and bundles that are managed by GIM, and to display and change any parameter for the bundles.

The configurator.sh script is installed with the GIM bundle on the database server, and is located in the UTILS folder.

The GIM and S-TAP clients do not need restarting after running this script.

The syntax is:

```
<GIM installation directory>/UTILS/current/files/bin/configurator.sh [--set <param name> <param value>| --get <module name> | -list | --delayed_bundle_deployment <enable|disable>
```

| Parameter | Description |
|------------------------------|--|
| delayed_bundle_deployment | <ul style="list-style-type: none">• <i>enable</i>: suspends any scheduled installations• <i>disable</i>: scheduled installations take place
Default = <i>disable</i> |
| get <module name> | Returns the value of all the parameters that are specified for the module. Modules are returned by the parameter list. |
| list | Lists all the GIM modules and their status. |
| set <parameter name> <value> | Set the module's parameter to the specified value. |

Examples:

- To list the GIM-managed modules and bundles, and their status:

```
/usr/local/IBM/modules/UTILS/current/files/bin/configurator.sh --list
[Wed Jan 20 08:58:56 2021] STAP-UTILS      11.1.0.11_r109779_1  INSTALLED
[Wed Jan 20 08:58:56 2021] SUPERVISOR      11.1.0.11_r109779_1  INSTALLED
[Wed Jan 20 08:58:56 2021] COMPONENTS       11.1.0.11_r109779_1  INSTALLED
[Wed Jan 20 08:58:56 2021] STAP           11.1.0.11_r109779_1  INSTALLED
[Wed Jan 20 08:58:56 2021] UTILS          11.1.0.11_r109779_1  INSTALLED
[Wed Jan 20 08:58:56 2021] BUNDLE-GIM     11.1.0.11_r109779_1  INSTALLED
[Wed Jan 20 08:58:56 2021] KTAP          11.1.0.11_r109779_1  INSTALLED
[Wed Jan 20 08:58:56 2021] GIM           11.1.0.11_r109779_1  INSTALLED
[Wed Jan 20 08:58:56 2021] BUNDLE-STAP    11.1.0.11_r109779_1  INSTALLED
[Wed Jan 20 08:58:56 2021] INIT          11.1.0.11_r109779_1  INSTALLED
[Wed Jan 20 08:58:56 2021] ATAP          11.1.0.11_r109779_1  INSTALLED
```

- To view the GIM parameter values:

```
/usr/local/IBM/modules/UTILS/current/files/bin/configurator.sh --get GIM
GIM_ALLOW_CUSTOMED_BUNDLES=0
GIM_ALLOW_IP_HOST_COMBO=0
GIM_AUTO_SET_CLIENT_IP=0
GIM_CA_FILE=gim_ca.pem
GIM_CERT_FILE=gimListenerServer.cert.pem
GIM_CLIENT_IP=nn.nnn.nnn.nnn
GIM_DEBUG=0
GIM_DISKSPACE=1000
GIM_ENABLED=1
GIM_FAILOVER_URL=
GIM_INTERVAL=60
GIM_KEY_FILE=gimListenerServer.key.pem
GIM_LISTENER_PORT=8445
GIM_PACKAGE=guard-GIM-11.1.0.11_r109779_v11_1_rhel-7-linux-x86_64.tar.gz.signed
GIM_PART_OF_BUNDLE=BUNDLE-GIM
GIM_RESPONSE_TIMEOUT=600
GIM_SYMVERSION=11.1.0.11_r109779_v11_1
GIM_URL=<server name>
GIM_URL_PORT=8081
GIM_URL_SSL_NO_AUTH_PORT=8444
GIM_URL_SSL_PORT=8446
GIM_USE_SSL=1
GIM_VERSION=11.1.0.11_r109779_1
COMMON_ALIVE_INTERVAL=900
COMMON_DEBUG=0
COMMON_INSTALL_DIR=/usr/local/IBM/modules
```

```

COMMON_OS=Linux
COMMON_OS_BITS=64
COMMON_OS_VENDOR=rhel
COMMON_OS_VENDOR_VERSION=7
COMMON_OS_VERSION=
COMMON_PATH=/usr/local/IBM/modules:/usr/xpg4/bin:/bin:/sbin:/usr/bin:/usr/local/bin:/usr/contrib/bin:
COMMON_PERL_DIR=/usr/bin
COMMON_PLATFORM_PROCESSOR=x86_64
COMMON_PROTOCOL_VERSION=100_r0_3

```

- To change the value of the GIM_URL parameter:
`/usr/local/IBM/modules/UTILS/current/files/bin/configurator.sh --set GIM_URL nn.nn.nn.nn`
- To disable any GIM upgrades from deploying:
`/usr/local/IBM/modules/UTILS/current/files/bin/configurator.sh --delayed_bundle_deployment enable`

GIM CLI commands

You can use the CLI to install and upgrade modules on the database server.

The following examples are presented only to cover some of the more common scenarios. For more information and a complete list of all supported CLI commands, see [Guardium Installation Manager \(GIM\) APIs](#).

- Loading module packages
- Upgrade or Scratch install by using bundles
- Uninstall a module or bundle
- Installation Status
- Querying modules state

Loading module packages

Before modules can be installed on DB server, they must be loaded onto the Central Manager GIM database. If a Central Manager is not part of the architecture, packages must be loaded onto each Guardium® system. Use the Load package option in the GIM UI to get the packages loaded to the database.

Upgrade or Scratch install by using bundles

Note: Scratch installation refers also to a case where old (pre-GIM) S-TAP is installed on the database server.

A bundle is a list of modules that are grouped for ease of installation. Always use bundles to install or upgrade modules.

1. Get the list of registered clients (database servers installed with GIM client that have registered with the GIM server):

```

grdapic gim_list_registered_clients
ID=0
##### ENTRY 0 #####
CLIENT_ID: 1
IP: 192.168.2.204
OS: HP-UX
OS_RELEASE: B.11.00
OS_VENDOR: hp
OS_VENDOR_VERSION: B.11.00
OS_BITS: 64
PROCESSOR: 9000
##### ENTRY 1 #####
CLIENT_ID: 2
IP: 192.168.2.210
OS: Linux
OS_RELEASE: 2.6.16.54-0.2.5-smp
OS_VENDOR: suse
OS_VENDOR_VERSION: 10.1
OS_BITS: 64
PROCESSOR: x86_64

```

2. Assign (prepare to install; NOT a request to install it on the client) the latest bundle available for a specific client:

```
grdapic gim_assign_latest_bundle_or_module_to_client clientIP=198.168.2.210 moduleName=BUNDLE-STAP
```

Note: To assign a specific bundle or module to a client, use this sequence:

```
gim_get_available_modules clientIP="client ip"
gim_assign_bundle_or_module_to_client_by_version clientIP="client ip" moduleName="Bundle/Module name"
moduleVersion="Bundle/Module version"
```

3. Schedule the installation.

```
grdapic gim_schedule_install clientIP=192.168.2.210 date=now
```

Note: For multiple client installation repeat steps 2-3.

Note: For flexible GIM scheduling, use now + [1-9][0-9]* minute | hour | day | week | month. Example: now + 1 day, now + 3 minutes

GIM scheduling

All time is relative to Guardium system time. Now means right now as specified by the Guardium system. Now +30 minutes is the current Guardium system time + 30 minutes. If the time on the database server has passed the time on the Guardium system that is specified for installation, then the installation begins.

Example one, set up three clients (a) set for Guardium system time - 1 hour, (b) set for Guardium system time, and (c) set for Guardium system time + 1 hour.

Set up an S-TAP installation by using GIM for "now +30 minutes".

Guardium system (a), which is already 30 minutes ahead of the time set for installation, installs immediately.

Guardium system (b) installs in 30 minutes.

Guardium system (c) takes another hour after (b) to install.

Example two - Same setup as example one but this time specify "now".

Installation status changes to IP immediately on all clients.

Uninstalling a module or bundle

```
grdapapi gim_uninstall_module clientIP=192.168.2.210 module=BUNDLE-STAP date=now
```

You can specify `date=now` or use the format of `YYYY-MM-DD HH:mm`. The uninstallation will take place the next time GIM client checks for updates (GIM_INTERVAL).

Installation Status

Additional information about the latest status the client sent can be retrieved by running the following command. (The status message appears as an entry in GIM_EVENTS table from which a report can be generated):

The general status message can be obtained by running the following CLI command:

```
grdapapi gim_get_client_last_event clientIP="client ip"
grdapapi gim_get_client_last_event clientIP=winx64
grdapapi gim_get_client_last_event clientIP=9.70.144.73
```

Sample output from this command:

```
ID=0
OK
BUNDLE-STAP-8.0_r2609_1 INSTALLED
STAP-UTILS-8.0_r2609_1 INSTALLED
COMPONENTS-8.0_r2609_1 INSTALLED
KTAP-8.0_r2609_1 INSTALLED
STAP-8.0_r2609_1 INSTALLED
TEE-8.0_r2609_1 INSTALLED
ATAP-8.0_r2609_1 INSTALLED
```

Querying modules state

To query the installed module's state per client, enter the following CLI command:

```
grdapapi gim_list_client_modules clientIP="client ip"
```

The following states are possible:

INSTALLED
Module is installed.

PENDING-INSTALL
Module is pending to be scheduled for installation.

PENDING-UNINSTALL
Module is pending to be scheduled for uninstallation.

PENDING-UPDATE
Module is pending to be scheduled for update.

IP
Module installation is in progress.

FAILED
Module's last operation failed.

IP-PR
Module requires client reboot to complete the installation process. Before rebooting, deactivate all A-TAP instances. Rebooting the database server is different per OS (Any other way of rebooting the system keeps the pending modules in a pending state).

- AIX: reboot
- Linux® shutdown -r
- SuSe: reboot
- HP-UX: shutdown -r
- Solaris: shutdown -i [6|0] (Note: '0' can be used only if shutdown is done from the terminal server)

Output example:

```
ID=0
##### ENTRY 0 #####
MODULE_ID: 11
NAME: INIT
INSTALLED_VERSION 8.0_r3852_1
SCHEDULED_VERSION 8.0_r3852_1
STATE: INSTALLED
IS_SCHEDULED: N
#####
ENTRY 1 #####
MODULE_ID: -1
NAME: COMMON
INSTALLED_VERSION 8.0_r0_1
SCHEDULED_VERSION 8.0_r0_1
```

```

STATE:           INSTALLED
IS_SCHEDULED:   N
##### ENTRY 2 #####
MODULE_ID:      12
NAME:            UTILS
INSTALLED_VERSION 8.0_r3852_1
SCHEDULED_VERSION 8.0_r3852_1
STATE:           INSTALLED
IS_SCHEDULED:   N
##### ENTRY 3 #####
MODULE_ID:      13
NAME:            SUPERVISOR
INSTALLED_VERSION 8.0_r3852_1
SCHEDULED_VERSION 8.0_r3852_1
STATE:           INSTALLED
IS_SCHEDULED:   N
##### ENTRY 4 #####
MODULE_ID:      14
NAME:            GIM
INSTALLED_VERSION 8.0_r3852_1
SCHEDULED_VERSION 8.0_r3852_1
STATE:           INSTALLED
IS_SCHEDULED:   N
##### ENTRY 5 #####
MODULE_ID:      15
NAME:            BUNDLE-GIM
INSTALLED_VERSION 8.0_r3852_1
SCHEDULED_VERSION 8.0_r3852_1
STATE:           INSTALLED
IS_SCHEDULED:   N

```

GIM user interfaces

The purpose of GIM is to provide automatic installation capability for modules, taking advantage of a GIM client residing on each database server and a GIM server on the Guardium® system.

Users may also interact with GIM through the CLI. See [GIM CLI commands](#) for information on installing and upgrading modules with GIM using CLI.

You can use the GUI of the Guardium Installation Manager (GIM) for these tasks:

- Process Monitoring
- Upload Module Package
- Configure, Install, or Update Modules
- Rollback Mechanism

Note: If A-TAP is being used, A-TAP must first be disabled on the database server before performing a GIM-based S-TAP upgrade or uninstall.

Note: GIM does not support the installation of native S-TAP installers (rpm, dept, bff, etc.)

Note: Installation of modules on a specific client for the FIRST TIME using the GIM utility must be in the form of a BUNDLE. Future upgrades of specific modules which are part of the installed bundle can be either as single modules or bundles.

GIM Processes

- Supervisor: The GIM Supervisor is a process with the main purpose of supervising and monitoring Guardium processes. Specifically, it is responsible for starting, stopping, and making sure all of Guardium processes are running at all times, and restarting them if they fail.
- GIM: The GIM process is the GIM client process, which is responsible for such duties as registering to the GIM server, initiate a request to check for software updates, installing the new software, updating module parameters, and uninstalling modules.

Commands for starting and stopping services are listed in [Linux-UNIX: Start and stop S-TAP and GIM processes for various OS types/versions](#).

GIM Processes Monitor page

This page displays the status of GIM processes on servers. You can filter for: up, down, unknown; or use the free text filter.

Configure, Install, or Update Modules

For information about the latest GIM software management tool, see [Set up by Client](#).

Windows S-TAP Parameters in GIM

During S-TAP installation, or to update the S-TAP configuration, you can use the WINSTAP_CMD_LINE field in the Setup by Client page.

You can input any parameter in the Setup by Client page, in the Choose parameters row, using the command WINSTAP_CMD_LINE with the syntax **parameter=value** for [TAP] parameters, or CLI parameters ([Windows: S-TAP command line installation parameters](#)) with the syntax **-param value**, and it is added or updated in the guard_tap.ini.

CAUTION:

There is no validation of input to this field.

For example, the following command line options skip the installation of CAS and Named Pipes support.

```
CAS=0 NamedPipes=0
```

If you are installing an S-TAP and you do not want it to automatically discover MSSQL databases, type **START=0** in the **WINSTAP_CMD_LINE** column to prevent the S-TAP from starting when it is installed. You can also specify this parameter for a single database server by using the GIM API:

```
grdapic Gim_update_client_params clientIP=xx.xx.xx.xx paramName=WINSTAP_CMD_LINE paramValue="START=0"
```

Additional guard_tap.ini parameters may also be set at installation. An example is **paramValue="START=1 !client_timeout_sec=120&use_tls=1!"**

Note: When using GuardAPI commands, the **WINSTAP_CMD_LINE** **paramValue** should be quoted and each parameter separated by spaces, such as **paramValue="START=1 CAS=0"** as in the prior example. A lack of spaces can cause the subsequent installation to not complete as anticipated.

Rollback Mechanism

GIM's rollback mechanism purpose is to handle errors during installation and recover modules to their prior state. The Rollback mechanism supports the following recovery scenarios:

1. Live Upgrade Recovery

For Bundles

- When bundles are installed, recovery will rollback the modules that have an install failure within the bundle.
- Modules that are marked as **NO_ROLLBACK** (in the form of a read-only parameter <MODULE>_NO_ROLLBACK=1) will not be rolled back in the event of a failure. S-TAP/KTAP are two such modules that once successfully installed will not be rolled back in the event of a failure of another module.

For non-Bundles

- Rollback entails the removal of the standalone module in the case of a scratch install or reverting back to the previous version in case of an upgrade.

2. Boot Time Installation Recovery

If installation failure occurs during a system reboot, a second system reboot will be needed in order to complete the recovery. Users will still see the status IP-PR after reboot, and a GIM_EVENT entry that indicates a second reboot is needed to complete the recovery process. The module/bundle state will then indicate a "FAILED" status after the second reboot.

Note: When the status is 'IP-PR' booting the DB-server is different per OS (Any other way of rebooting the system will keep the pending modules in a pending state):

```
Linux   : shutdown -r
SuSe   : reboot
HP     : shutdown -r
Solaris : shutdown -i [6|0]  (Note : '0' can be used only if shutdown is done from the terminal server)
AIX    : reboot
Tru64  : reboot
```

Note: In addition, prior to reboot, A-TAP instances must be disabled/deactivated.

Distributing GIM bundles to managed units

You can distribute GIM bundles to managed units in order to deploy them on the GIM clients managed by those managed units.

About this task

If you manage all your GIM clients from your Central Manager, you can deploy bundles to all your GIM clients directly from the Central Manager. If you manage groups of clients from several managed units, you can distribute GIM bundles from your central manager to those managed units.

The time required for distribution depends on the size of the bundles and network conditions. In a network with substantial latency, transfers can take several hours.

Procedure

1. Copy the bundles that you want to distribute into the **/var/gim/dist_packages** directory on your Central Manager. All files in this directory will be distributed; you cannot select which bundles you want to distribute.
2. Choose the managed units to which you want to distribute the bundles.
3. Click Distribute GIM bundles.

The bundles are copied to the selected managed units.

Results

You can install the bundles from each managed unit to the GIM clients that it manages.

Removing unused GIM bundles

You can remove GIM bundles from your GIM server if they are no longer used on any database server.

About this task

This function enables you to maintain your inventory of GIM bundles and prevent it from using disk space unnecessarily.

You can use two new Guardium API commands to identify and remove unused GIM bundles. Perform this procedure on each Guardium system that acts as a GIM server.

Procedure

1. Run the **gim_list_unused_bundles** command to identify unused bundles for FAM install. Use the **includeLatest** parameter to indicate whether you want the list that is returned by the command to include the latest version of each GIM bundle. You might have some bundles that you have not yet distributed, or you might want to

keep one older version so that you can reinstall it if needed. Set includeLatest to 0 to exclude the latest unused version of each bundle from the command results. Set it to 1 to include all unused versions. This parameter is required and no default value is provided. For example:

```
gim_list_unused_bundles includeLatest=0
```

The command returns a list of GIM bundles that are found on the GIM server but are not installed on any database server whose GIM client works with this GIM server.

2. If step 1 identifies some unused bundles, use the **gim_remove_bundle** command to remove each unwanted bundle. This command takes a single parameter, bundlePackageName, which identifies the bundle to be removed. This parameter is required and no default value is provided. Use names that are returned by the **gim_list_unused_bundles** command.

The named bundle is removed only if:

- The name specified in bundlePackageName matches the name of one and only one specific GIM bundle.
- There is no GIM bundle whose name matches bundlePackageName installed on any database server whose GIM client works with this GIM server.

For example:

```
gim_remove_bundle bundlePackageName=name
```

where name is a bundle name that was returned by the **gim_list_unused_bundles** command.

Results

GIM bundles that are not needed are removed from your GIM server.

Starting and restarting GIM services and components

- [Restarting the supervisor for Solaris with SMF support](#)

Use a set of CLI commands to restart the supervisor on Solaris servers with SMF support.

Restarting the supervisor for Solaris with SMF support

Use a set of CLI commands to restart the supervisor on Solaris servers with SMF support.

About this task

To restart the supervisor, complete the following procedure. Only use this procedure on Solaris servers with SMF support.

Procedure

1. Stop the supervisor by running the command **svcadm -v disable guard_gsvr**.
2. Run the command **svccfg delete -f guard_gsvr**.
3. Restart the supervisor with the command **svccfg import <gim install dir>/SUPervisor/current/guard_gsvr.xml** where **<gim install dir>** is the file path to the GIM installation directory.

Results

The supervisor is restarted for Solaris with SMF support.

Installing your Guardium Data Protection system

This document details the steps necessary to install and configure your IBM® Guardium system.

This document also provides information on how to customize the partitioning on the appliance and how to install on a remote drive (SAN).

The steps are:

1. Assemble configuration information and the hardware required before you begin.
2. Set up the physical appliance or the virtual appliance.
3. Install the Guardium image.
4. Set up initial and basic configurations.
5. Verify successful installation.

The IBM Guardium solution is available as:

- Hardware offering – a fully configured software solution delivered on physical appliances provided by IBM.
- Software offering – the solution delivered as software images to be deployed by the customers on their own hardware either directly or as virtual appliances.

The requirements listed in this document apply to the installation of both the physical appliance and the virtual appliance unless specified otherwise.

- [Operating modes](#)

You can deploy a Guardium system in any of several operating modes.

- [License keys](#)

Establishing a functional Guardium system requires both a base license and one or more append licenses.

- [Hardware Requirements](#)
Detailed hardware requirements and sizing recommendations are available on the IBM Support Portal.
- [Guardium port requirements](#)
Each Guardium system must have ports available for several types of communication. This section lists these connections and the default port numbers that are assigned to them.
- [Step 1. Assemble the following before you begin](#)
To prepare for the deployment of the Guardium system, the network administrator needs to supply the following information.
- [Step 2. Set up the physical or virtual appliance](#)
The setup instructions in this section are different when installing to a physical appliance or a virtual appliance.
- [Step 3. Install the Guardium image](#)
This section explains how to install the image and partition the disk.
- [Step 4. Set up initial and basic configuration](#)
The initial step should be the network configuration, which must be done locally through the Command Line Interface (CLI) accessible through the serial port or the system console.
- [Step 5. What to do next](#)
This section details the steps of verifying the installation, installing license keys, and installing any available maintenance patches.
- [Creating the Virtual Image](#)
Use this section to install the virtual image.
- [Custom Partitioning](#)
If you customize the partitioning of the hard drive, you must make several choices.
- [How to partition with an encrypted LVM](#)
If you use an encrypted disk, create an encrypted LVM volume that contains the / and /var logical volumes.
- [Create an LVM disk with four disks](#)
- [Example of SAN Configuration](#)
This appendix details the steps involved in moving to a command prompt in order to pre-partition a hard drive (as is needed for SAN installation).

Operating modes

You can deploy a Guardium® system in any of several operating modes.

As you plan your Guardium environment, you might deploy systems in any or all of these operating modes:

Collector

A collector receives data about database activities or file activities from agents that are deployed on database servers and file servers. The collector processes this data and responds according to policies that are installed on the collector. A collector can export data to an aggregator.

Aggregator

An aggregator collects data from several collectors, to provide an aggregated view of the data. The aggregator is not connected directly to database servers and file servers. You can allocate collectors to aggregators according to location or function. For example, you might want to connect the collectors that monitor your human resources database servers to a single aggregator, so that you can view data that is related to all those servers in one location. If you want, you can implement a second tier of aggregation by deploying an aggregator that collects data from all your other aggregators, rather than from collectors.

Note: If you plan to use the appliance as a central manager you MUST select Aggregator option.

Central manager

There is only one central manager in a Guardium environment, although you can designate another Guardium system as a backup central manager. You can use the central manager to define policies and distribute them to all collectors, to perform other configuration tasks that affect all your Guardium systems, and to perform various other administrative tasks from a single console. Your central manager can also function as an aggregator, collecting data from collectors or from other aggregators. This model provides an enterprise-wide view of activities and enables you to view reports that are based on data that is aggregated from all your Guardium systems.

The number of monitored database servers and file servers that you assign to a collector depends on the amount of data that flows from the servers to the collector. For information about how many collectors and aggregators your environment requires, and how to locate your Guardium systems for best results, refer to the [Deployment Guide for IBM® Guardium](#).

If you are using the Guardium Vulnerability Assessment component, you must decide where to run assessment tests. Some customers dedicate a separate Guardium system for this function. You can also run tests from any Guardium system that is deployed as a collector, an aggregator, or a central manager.

License keys

Establishing a functional Guardium® system requires both a base license and one or more append licenses.

Base and append licenses are described as follows:

- Base license keys (also known as reset keys) reflect the machine type of the system. For example, establishing collector system requires a collector base license.
- Append license keys enable specific sets of features. For example, typical data activity monitoring features require a DAM Standard append license. Multiple append licenses can be installed in combination to enable expanded Guardium functionality.

When applying a base license, the machine type is checked to verify compatibility. There are two types of base licenses:

Table 1. Base license types

| Base License Type | License Description |
|-------------------|---|
| Collector | Collector base licenses are valid for establishing a standalone system or a collector. |
| Aggregator | Aggregator base licenses are valid when establishing an aggregator or a central manager system. |

The features available on your Guardium system depend on the append license(s) you have installed. The following append licenses are available and can be used in combination:

Table 2. Append license types

| Append License Type | License Description |
|---------------------|---------------------|
|---------------------|---------------------|

| Append License Type | License Description |
|---------------------|---|
| DAM Standard | Core functionality for data activity monitoring. |
| DAM Advanced | DAM Standard functionality plus fine-grained access control, masking, quarantine, and blocking (activity terminate). |
| FAM Standard | Core functionality for file activity monitoring. |
| FAM Advanced | FAM Standard functionality plus blocking. |
| VA Standard | Vulnerability assessment plus database protection service (DPS), change audit system (CAS), and database entitlement reporting. |

For information about installing Guardium licenses, see [Install license keys](#).

Related tasks

- [Install license keys](#)

Hardware Requirements

Detailed hardware requirements and sizing recommendations are available on the IBM Support Portal.

For detailed hardware specifications and sizing recommendations, refer to [Hardware requirements](#).

Guardium port requirements

Each Guardium® system must have ports available for several types of communication. This section lists these connections and the default port numbers that are assigned to them.

Open ports

Ports that are used in or by the Guardium system.

DB Server – Collector

- TCP 8443 - open from DB server to collector
- TCP 16016 – UNIX STAP, both directions, registration, heartbeat, and data (including IBM i S-TAP running in PASE)
- TCP 16017 – Windows/Unix CAS, both directions, templates and data
- TCP 16018 – UNIX S-TAP (TLS) and External S-TAP, both directions, registration, heartbeat, and data
- TCP 16019 – Windows/Unix CAS (TLS), both directions, templates and data
- TCP 16020 - From S-TAP agent Clear UNIX S-TAP connection pooling
- TLS 16021 - From S-TAP agent Encrypted UNIX S-TAP connection pooling
- TCP 8081 – Guardium Installation Manager, both directions, database server to collector/Central Manager
- TCP 9800 – Windows S-TAP using protocol 8, both directions, DB Server to Collector, S-TAP registration and data
- TCP 9801 – Encrypted (TLS) Windows S-TAP using protocol 8, both directions, DB Server to Collector, S-TAP registration and data

Collector – Aggregator (Secure Shell – SSL)

- TCP 22 – collector to aggregator, SCP data exports, both directions

Central Manager – Managed Devices

- TCP 22 – SSH/SCP data transfers, both directions
- TCP 8443 – SSL, both directions
- TCP 8444 – SSL, STAP to GIM file upload
- TCP 3306 – MySQL, opened to specific sources (for instance, the Central Manager is open to all managed units; a managed unit is open to the Central Manager)
- TLS 8447 - Used for remote messaging service infrastructure (and profile distribution infrastructure) for communication between Guardium systems in the federated environment / centrally-managed environment. Configuration profiles allow the definition of configuration and scheduling settings from a Central Manager and conveniently distribute those settings to managed unit groups without altering the configuration of the Central Manager itself.
- TCP 8983 –Apache Solr Index. Used for establishing communication between the Central Manager and every Managed Unit, as well as between each Managed Unit and the Central Manager that is required in default mode. Communication between all the Managed Units is required only in the 'all machines' mode.
- TCP 9983 –Apache Solr Index. Establish communication in between Managed Units and Central Manager. Both directions.

File Activity Monitoring (FAM), on the unit where it is installed. (Bidirectional means data can be sent or received in both directions once connection is established.)

- TCP/TLS 16022/16023: Universal Feed. 16022 (FAM monitoring, unencrypted) and 16023 (FAM monitoring, encrypted) both need to be open bidirectionally.
- 16016 to 16023: These ports must be open bidirectionally for the sniffer. The connection is made from the S-TAP to the sniffer (sniffer does not initiate the connection); listening ports are on the sniffer side only.
- 18087: Listener port for FAM on IBM Content Classification (ICM) server located on the same machine where FAM is installed.
(serverSettings.icmURL=http://localhost:18087) Open bidirectionally.

Guardium Installation Manager (GIM)

- 8445 - GIM client listener, both directions. The GIM client is doing the listening. Any GIM server on either the Central Manager or the collector can reach out to it the GIM client.
- 8446 - GIM authenticated TLS, both directions. Use between the GIM client and the GIM server (on the Central Manager or collector). If GIM_USE_SSL is NOT disabled, then the gim_client will attempt to communicate its certificate via port 8446. IF port 8446 is NOT open, then it defaults to 8444, BUT no certificate is passed (for example, TLS without verification).
- 8081 - TLS - To use 8081 for the GIM client to connect to the GIM server, there is a need to disable the GIM_USE_SSL parameter - it is ON by default. This parameter is part of the GIM common parameters in the GUI. If GIM_USE_SSL is NOT disabled, then the gim_client will attempt to communicate its certificate via port 8446. IF port 8446 is NOT open, then it defaults to 8444, BUT no certificate is passed (for example, TLS without verification).

Enterprise load balancer

- TLS 8443 - S-TAP load balancer - This is needed for UNIX/Linux S-TAPs to communicate instances to the collector. However this port is also used for the Central Manager load balancer. The S-TAP initiates a request to central manager (load balancer) on 8443 sending HTTPS message, if installation indicates to use Enterprise load balancer. Between the database server and central manager, there will be the capability to use a proxy server, if customer doesn't want an open port directly from database to central manager.

User Interface - Guardium System (standalone, aggregator, central manager)

- TCP 22 - user to system, CLI connectivity, both directions
- TCP 8443 - user to system, GUI connectivity (configurable), both directions, sending discovered instances to the UI
- 8445 - TLS. Bidirectional port to connect to a file server.

System – SMTP server

- TCP 25 – system to SMTP server, email alerts

System – SNMP server

- UDP 161 - SNMP client to system – SNMP Polling
- UDP 162 - system to SNMP server, SNMP traps

System – SYSLOG server

- UDP/TCP 514 – remote syslog message from/to other systems, typically SIEM
Note: The local port is 514, but the remote port must be entered into the configuration. If encryption is used, the protocol must be TCP, not UDP.

System – NTP server

- UDP 323 – system to Network Time Protocol Server

System – DNS server

- TCP/UDP 53 – system to Domain Name Server

System – EMC Centera (backups)

- TCP 3218 – system to EMC Centera

System – Tivoli LDAP

- UDP 389 – system to/from Tivoli LDAP

System – Mainframe

- TCP 16022 – connects S-TAP to DB2 z/OS, S-TAP IMS, S-TAP VSAM (S-TAP Data Set)
- TCP 16023 - TLS connections, specifically IBM's Application Transparent Transport Layer Security (AT-TLS)

Outbound ports to monitor Azure streaming

The following ports must be open to support IPv4 connections to Azure services.

| Port | Protocol | Purpose |
|------------|----------|-----------------|
| 443 | SSL | Azure Namespace |
| 5671, 5672 | AMQP | Azure Namespace |
| 443 | SSL | Azure Storage |

Outbound ports to monitor AWS streaming

The following ports must be open to support IPv4 connections to AWS.

| Port | Protocol | Purpose |
|------|----------|--|
| 443 | SSL | AWS Kinesis, AWS DynamoDB, AWS CloudWatch, and AWS KMS |

Ports for connections to Windows database servers

| Port | Protocol | Purpose |
|-------|----------|--|
| 9500 | TCP | Clear Windows S-TAP |
| 9501 | TLS | Encrypted Windows S-TAP (optional) |
| 16017 | TCP | Clear Windows CAS |
| 16019 | TLS | Encrypted Windows CAS (optional) |
| 9800 | TCP | Windows S-TAP using protocol 8, both directions, DB Server to Collector, S-TAP registration and data |
| 9801 | TLS | Encrypted (TLS) Windows S-TAP using protocol 8, both directions, DB Server to Collector, S-TAP registration and data |

Default ports used for Guardium Application Access

| Port | Protocol | Purpose |
|------|----------|---------|
| | | |

| Port | Protocol | Purpose |
|------|----------|--|
| 8443 | TCP | <p>The port is used for:</p> <ul style="list-style-type: none"> • Web browser access (https) to the Guardium user interface. • Registering a managed unit to a central manager. • Checking connectivity between aggregators or central managers and collectors. <p>Note: Change this port using the HTTPS Port setting available at Setup > Tools and Views > Portal.</p> |
| 22 | TCP | SSH access from clients to manage the Guardium appliance |
| 3306 | TCP | Communication between central manager and managed units |

Ports for connections to z/OS database servers

| Port | Protocol | Purpose |
|-------|----------|---|
| 16022 | TCP | Connects to S-TAP for DB2 z/OS, S-TAP for IMS, S-TAP for Data Sets |
| 16023 | TCP | TLS connections, specifically IBM's Application Transport Layer Security (AT-TLS) |
| 41500 | TCP | Default starting port for internal message logging communications – LOG_PORT_SCAN_START |
| 39987 | TCP | Default agent-specific communications port between the agent and the agent secondary address spaces – ADS_LISTENER_PORT |

Default ports used for other features

| Port | Protocol | Purpose |
|--------------|----------|---|
| 20, 21 | TCP | FTP Server for backups/archiving (optional) |
| 22 | TCP | SCP for backups/archiving, patch distributions, and file-transfers |
| 25 | TCP | SMTP (email server) for alerts and other notification |
| 53 | TCP | DNS Servers |
| 123 | TCP, UDP | NTP (Time Server) for time synchronization |
| 161 | TCP, UDP | SNMP Polling (optional) |
| 162 | TCP, UDP | SNMP Traps (optional) |
| 389 | TCP | LDAP, for example, Active Directory or Sun One Directory |
| 443 | TCP | Default outbound port from External S-TAP® GUI to Kubernetes API |
| 514 | TCP | Syslog Server (optional) |
| 636 | TCP | LDAP, for example, Active Directory or Sun One Directory over SSL (optional) |
| 1500 | TCP | Tivoli Storage Manager backup hosts (optional) |
| 3218 | TCP, UDP | EMC Centera backup hosts (optional) |
| user-defined | TCP | Database Server listener ports, for example, 1521 for Oracle or 1433 for MS-SQL, for Guardium datasource access (optional). Use this port for S-TAP verification and Discovery. |
| 16022/16023 | TCP/TLS | Universal Feed - File Activity Monitoring (FAM0) |
| 18027 | | FAM using IBM Content Classification locally (serverSettings.icmURL=http://localhost:18087) |
| 8445 | | GIM client listener, both directions

The GIM client is doing the listening. Any GIM server on either the central manager or the collector can reach out to it (the GIM client). |
| 8446 | TLS | GIM authenticated TLS, both directions

Use between the GIM client and the GIM server (on the central manager or collector).

If GIM_USE_SSL is NOT disabled, then the gim_client will attempt to communicate its certificate via port 8446. If port 8446 is NOT open, then it defaults to 8444 BUT no certificate is passed (for example, TLS without verification). |
| 8447 | TLS | Used for remote messaging service infrastructure (and profile distribution infrastructure) for communication between Guardium systems in the federated environment / centrally-managed environment. Configuration profiles allow the definition of configuration and scheduling settings from a central manager and conveniently distribute those settings to managed unit groups without altering the configuration of the central manager itself. |
| 8443 | TLS | Enterprise load balancer

This is needed for UNIX/Linux S-TAPs to communicate instances to the collector.

However, this port is also used for the central manager load balancer. If the installation wants to use Enterprise load balancer, then the S-TAP initiates a request to the central manager on port 8443 by sending an HTTPS message.

So, between database server and central manager, there will be the capability to use a proxy server, if customer doesn't want an open port directly from database to central manager. |
| 8081 | TLS | To use 8081 for the GIM client to connect to the GIM server - need to disable the GIM_USE_SSL parameter - it is ON by default. This parameter is part of the GIM common parameters in the GUI. If GIM_USE_SSL is NOT disabled, then the gim_client will attempt to communicate its certificate via port 8446. If port 8446 is NOT open, then it defaults to 8444 BUT no certificate is passed (for example, TLS without verification). |
| 8983 | TCP | Used for establishing communication between the Central Manager and every Managed Unit, as well as between each Managed Unit and the Central Manager that is required in default mode.

Communication between all Managed Units is required only in 'all machines' mode. |
| 9983 | TCP | Used for establishing communication from the Managed Unit to the Central Manager. |

Related reference

- [Cipher suites](#)

Step 1. Assemble the following before you begin

To prepare for the deployment of the Guardium® system, the network administrator needs to supply the following information.

- IP address for the interface card (the primary interface)
- Subnet mask for primary IP address
- Default router IP address.
- Hostname and domain name to assign to system
- DNS server IP addresses (up to three addresses), and add the new Guardium system to your DNS domain
- (optional) IP address for secondary management interface
- (optional) Mask for secondary IP management interface
- (optional) Gateway for secondary IP management interface
- (optional) NTP server hostname
- (optional) SMTP configuration information (for email alerts): IP address, port, and if authentication is used, an SMTP user name and password
- (optional) SNMP configuration information (for SNMP alerts) the IP address of the SNMP server and the trap community name to use.
- **[SAN storage devices](#)**
If the installation is to be deployed on a Storage Area Network (SAN), all configuration information needed by the SAN, must be prepared before deployment. Also, there are additional installation steps required to partition the SAN storage device and install the Guardium OS.

SAN storage devices

If the installation is to be deployed on a Storage Area Network (SAN), all configuration information needed by the SAN, must be prepared before deployment. Also, there are additional installation steps required to partition the SAN storage device and install the Guardium® OS.

Note: Installation on a SAN is supported, installation on a NAS is not supported.

Step 2. Set up the physical or virtual appliance

The setup instructions in this section are different when installing to a physical appliance or a virtual appliance.

- **[Physical Appliance](#)**
After the appliance has been loaded into the customer's rack, connect the appliance to the network in the following manner:
- **[Identify network ports](#)**
Use the following CLI commands to map the network ports.
- **[Default passwords for physical appliances](#)**
Default passwords are supplied for predefined users.
- **[Virtual appliance](#)**
The IBM Guardium Virtual Machine (VM) is a software-only solution licensed and installed on a guest virtual machine such as VMware ESX Server.

Physical Appliance

After the appliance has been loaded into the customer's rack, connect the appliance to the network in the following manner:

1. Find the power connections. Plug the appropriate power cord(s) into these connections.
2. Connect the network cable to the primary interface network port. Connect any optional secondary network cables.
3. Connect a Keyboard, Video and Mouse directly or through a KVM connection (either serial or through the USB port) to the system.
4. Power up the system.

Related information

-  [Lenovo System x3550 M5 Installation and Service Guide](#)
-  [Changes in eth0 management port](#)

Identify network ports

Use the following CLI commands to map the network ports.

show network interface inventory

Use this CLI command to display the port names and MAC addresses of all installed network interfaces.

```
show network interface inventory
Current network card configuration:
Device          | Mac Address           | Member of
ens4f1np1      | 84:16:0C:AA:36:ED    | br3
ens4f2np2      | 84:16:0C:AA:36:EE    | br4
```

```

ens4f3np3      | 84:16:0C:AA:36:EF      | br5
ens2f1         | B4:96:91:F7:D1:6D.     | br1
ens4f0np0      | 84:16:0C:AA:36:EC.      |
ens2f0         | B4:96:91:F7:D1:6C       | br0
ok

```

show network interface role

Use this CLI command to display the network port that is assigned as the primary port.

```

show network interface role
Device:          Role:
ens2f0           bridgemember
ens2f1           bridgemember
ens4f0np0        primary
ens4f1np1        bridgemember
ens4f2np2        bridgemember
ens4f3np3        bridgemember
br3              -
br4              -
br5              -
br1              -
br0              -
ok

```

The port ens4f0np0 is assigned as the primary port.

show network interface port

This command flashes the light 20 times on the physical port. Use this CLI command to locate a physical connector on the back of the appliance.

```
show network interface port ens4f0np0
```

The light on port ens4f0np0 flashes 20 times.

Install the software directly on a dedicated computer

When you install the Guardium software directly to disk on a dedicated computer, use the Physical appliance instructions.

Default passwords for physical appliances

Default passwords are supplied for predefined users.

When you receive a physical appliance from IBM, use these passwords for your initial configuration.

Note: Be sure to change all default passwords when you complete the installation.

Table 1. Default passwords for predefined users

| User | Default password |
|-----------|------------------|
| accessmgr | guard1accessmgr |
| admin | guard1admin |
| cli | guard1cli |

Virtual appliance

The IBM® Guardium® Virtual Machine (VM) is a software-only solution licensed and installed on a guest virtual machine such as VMware ESX Server.

To install the Guardium VM, follow the steps in Creating the Virtual Image. The steps are:

- Verify system compatibility
- Install VMware ESX Server
- Connect network cables
- Configure the VM Management Portal
- Create a new Virtual Machine
- Install the IBM Guardium virtual appliance

After installing the VM, return to Step 4, Setup Initial and Basic Configuration, for further instructions on how to configure your Guardium system.

Step 3. Install the Guardium image

This section explains how to install the image and partition the disk.

1. Make sure your UEFI/BIOS “boot sequence” settings are set to attempt startup from the removable media (the CD/DVD drive) before using the hard drive.
Note: Installation can take place from DVD. If needed, get the UEFI/BIOS password from Technical Support.
2. Load the Guardium® image from the installation DVD.

3. The following two options appear:

Standard Installation: this is the default. Use this choice in most cases when partitioning the disk.

Custom Partition Installation: allows more customization of all partitions (locally or on a SAN disk). See Custom partitioning for further information on how to implement this option.

Note:

- The Standard Installation wipes the disk, repartitions and reformats the disk, and installs a new operating system.
- On the first boot after installation, the user is asked to accept a Licensing Agreement. They can use PgDn to read through the agreement or Q to skip to the end. To accept the terms of the agreement, enter q to exit and then type yes. The user must enter yes to the agreement or the machine will not boot up.

4. The system boots up from DVD. It takes about 12 minutes for this installation.

(d) The installation process will now ask you to choose a collector or aggregator (will be set to "Collector" automatically after 10 seconds if no input is provided). See the Product Overview for an explanation of Collector and Aggregator. If you wanted to choose aggregator and you did not choose it within 10 seconds, you must reinstall in order to get back to this point where you have a choice of aggregator.

Note: If you plan to use the appliance as a central manager you MUST select Aggregator option.

5. The system automatically reboots at this point to complete the installation. The first login after a reboot requires a changing of passwords.

Step 4. Set up initial and basic configuration

The initial step should be the network configuration, which must be done locally through the Command Line Interface (CLI) accessible through the serial port or the system console.

In the following steps, you will supply various network parameters to integrate the Guardium® system into your environment, using CLI commands.

In the CLI syntax, variables are indicated by angled brackets, for example: <ip_address>

Replace each variable with the appropriate value for your network and installation. Do not include the brackets.

- **[Set the primary and secondary system IP addresses](#)**

Define the primary and secondary interfaces. Use these commands to specify the primary interface:

- **[Set the Default Router IP Address](#)**

Use the following CLI command:

- **[Set DNS Server IP Address](#)**

Set the IP address of one or more DNS servers to be used by the appliance to resolve host names and IP addresses. The first resolver is required, the others are optional.

- **[SMTP Server](#)**

An SMTP server is required to send system alerts. Enter the following commands to set your SMTP server IP address, set a return address for messages, and enable SMTP alerts on startup.

- **[Set Host and Domain Names](#)**

Configure the hostname and domain name of the appliance. This name should match the hostname registered for the appliance in the DNS server.

- **[Set the Time Zone, Date and Time](#)**

There are options for setting the date and time for the appliance.

- **[Set the Initial Unit Type](#)**

An appliance can be a standalone unit, a manager or a managed unit; In addition, an appliance can be set to capture database activity via network inspection or S-TAP or both. The standard configuration would be for a standalone appliance (for all appliances), and the most common setting would use S-TAP capturing (only for collectors).

- **[Resetting the root password](#)**

To reset your root password on the appliance, use your own private passkey and run the `support reset-password root` CLI command.

- **[Validate All Settings](#)**

Before logging out of CLI and progressing to the next configuration step, review and validate the configured settings using the following commands:

- **[Reboot the System](#)**

If the system is not in its final location, now is a good time to shut down the system, place it in its final network location, and start it up again.

Set the primary and secondary system IP addresses

Define the primary and secondary interfaces. Use these commands to specify the primary interface:

```
store network interface ip <ip_address>
store network interface mask <subnet_mask>
```

The default network interface mask is 255.255.255.0. If this value is the correct mask for your network, you can skip the second command.

To assign a secondary IP address, use the CLI command, **store network interface secondary** [on <interface> <ip> <mask> <gw> | off], that can be used to enable/disable the secondary interface. The secondary IP can not be in the same subnet as the primary interface IP. Assigning a secondary IP address can only be done using the CLI (and not the GUI).

Next, you must restart the network by using the CLI command, **restart network**.

The remaining network interface cards on the appliance can be used to monitor database traffic, and do not have assigned IP addresses.

Set the Default Router IP Address

Use the following CLI command:

```
store network routes defaultroute <default_router_ip>
```

Set DNS Server IP Address

Set the IP address of one or more DNS servers to be used by the appliance to resolve host names and IP addresses. The first resolver is required, the others are optional.

```
store network resolvers <IP address of resolver 1 [IP address of resolver 2] [IP address of resolver 3 ]>
```

For more information, see [Store network resolvers](#).

SMTP Server

An SMTP server is required to send system alerts. Enter the following commands to set your SMTP server IP address, set a return address for messages, and enable SMTP alerts on startup.

```
store alerter smtp relay <smtp_server_ip>
store alerter smtp returnaddr <first.last@company.com>
store alerter state startup on
```

Note: You can also configure the SMTP server by using the user interface. Click [Setup > Alerter](#).

Set Host and Domain Names

Configure the hostname and domain name of the appliance. This name should match the hostname registered for the appliance in the DNS server.

```
store system hostname <host_name>
store system domain <domain_name>
```

Set the Time Zone, Date and Time

There are options for setting the date and time for the appliance.

Timezone, date, time and Network

1. Set timezone
2. Set date and time
 - Option 1 - Set the Network Time Protocol (NTP) time server.
 - Option 2 - Store the system clock datetime.

Date/Time Option 1: Network Time Protocol

Provide the details for one or more accessible time servers (NTP) and then start the time server. As of Guardium 12.0, Guardium uses the chrony daemon to manage NTP servers.

```
store system time_server hostnames
store system time_server state on
```

Date/Time Option 2: Set the time zone, date and time

Use the following command to display a list of valid time zones:

```
store system clock timezone list
```

Choose the appropriate time zone from the list and use the same command to set it.

```
store system clock timezone <selected time zone>
```

Note: Setting up a new timezone restarts internal services. Data monitoring is disabled for a few minutes during this restart.

Store the date and time, in the format: YYYY-mm-dd hh:mm:ss

```
store system clock datetime <date_time>
```

Note: Do not change the hostname and the time zone in the same CLI session.

Set the Initial Unit Type

An appliance can be a standalone unit, a manager or a managed unit; In addition, an appliance can be set to capture database activity via network inspection or S-TAP or both. The standard configuration would be for a standalone appliance (for all appliances), and the most common setting would use S-TAP capturing (only for collectors).

store unit type standalone - use this command for all appliances.

store unit type stap - use this command for collectors.

Unit type standalone and unit type stap are set by default. Unit type manager (if needed) must be specified.

Note: Unit type settings can be done at a later stage, when the appliance is fully operational.

Resetting the root password

To reset your root password on the appliance, use your own private passkey and run the **support reset-password root** CLI command.

Note: The **support reset-password root** command requires the access key *t0Tach*.

Save the passkey used in your documentation to allow future Technical Support root accessibility. To see the current pass key, use the following CLI command:

```
support show passkey root
```

Questions - How secure is the Guardium system root password? Who has access to it?

For Guardium appliances, end users can use limited access operating system accounts, such as *cli* and *guardcli1* to *guardcli9*.

The GUI user accounts (such as admin and accessmgr) are not defined by the Guardium system's operating system, but are application IDs defined and managed from the accessmgr application interface.

Being a secured server, root access is not readily available to anyone. Root access is often required by Guardium support to gain access to the Guardium appliances to troubleshoot and resolve issues. Guardium support does not use sudo, or any other user ID other than root, to gain access to Guardium appliances.

The root password is secured by using a "joint password" mechanism. Your site holds the keys to the appliance in the form of an encoded numeric passkey. IBM holds the passkey decoder. For either you or IBM to access the appliance as root, both the passkey and passkey decoder are required.

You can manage the passkey from the CLI interface. You can change the passkey at any time, without notifying IBM, by using the following CLI command:

```
support reset-password root
```

Anyone with CLI access can retrieve the passkey for root by using the following CLI command:

```
support show passkey root
```

If you need to work with Guardium support on a remote desktop sharing session, the support analyst requests the root passkey for the Guardium appliance in question. After the passkey is decoded, Guardium support uses the root password to gain access to the appliance as root. After the remote desktop session ends, be sure to change the passkey (by using **support reset-password root**) to ensure that IBM no longer has the root password for this appliance.

All encoded passwords are hardened. They do not contain any common passwords or dictionary words, their length varies and they might contain national, special, and alphanumeric characters.

Access to the passkey decoder is restricted to a select few IBM Guardium employees, such as Guardium R&D, Guardium QA, and Guardium support staff members. It is not available to IBM staff.

The CLI user IDs (*cli*, *guardcli1* to *guardcli9*) do not use the passkey mechanism. Their passwords are entirely governed by your organization and IBM does not have access to their passwords. IBM recommends that you keep the root passkey in a password vault. This action ensures that you can access the appliance even if users at your site leave or misplace the CLI account passwords.

Validate All Settings

Before logging out of CLI and progressing to the next configuration step, review and validate the configured settings using the following commands:

```
show network interface all  
show network routes defaultroute  
show network resolver all  
show system hostname  
show system domain  
show system clock timezone  
show system clock datetime  
show system time_server all  
show unit type
```

Reboot the System

If the system is not in its final location, now is a good time to shut down the system, place it in its final network location, and start it up again.

Remove the installation DVD before you reboot the system.

To stop the system, enter the following command in the CLI:

```
stop system
```

The system shuts down. Move the system to its final location, re-cable the system, and power the system back on. After the system is powered on, it is accessible (using the CLI and GUI) through the network, using the provided IP address or host name.

Step 5. What to do next

This section details the steps of verifying the installation, installing license keys, and installing any available maintenance patches.

- **[Verify Successful Installation](#)**
Verify the installation by following the following steps:
- **[Set Unit Type](#)**
To set up a federated environment, configure one of the appliances as the central manager and set all the other appliances to be managed by the central manager.
- **[Install license keys](#)**
This topic guides you through the procedure of installing and accepting Guardium license keys.
- **[Install maintenance patches \(if available\)](#)**
You can install patches by using the CLI or through the GUI.
- **[Additional Steps \(optional\)](#)**
The following sections discuss changing the baseline English to another language, installing S-TAP® agents, defining Inspection Engines and installing CAS agents.

Verify Successful Installation

Verify the installation by following the following steps:

1. Login to CLI - ssh cli@<ip of appliance>
2. Login to GUI - https://<hostname of appliance>.<full domain>:8443 (use admin userid)

The first login after a reboot will require a changing of passwords.

Login to the Guardium web-based interface and go to the embedded online help for more information on any of the following tasks.

Set Unit Type

To set up a federated environment, configure one of the appliances as the central manager and set all the other appliances to be managed by the central manager.

Use the CLI command **store unit type** to set the type of each Guardium system.

Install license keys

This topic guides you through the procedure of installing and accepting Guardium® license keys.

Before you begin

- Download your license keys from Passport Advantage
- Install or upgrade your Guardium system
- Verify that the machine type is correctly set for your system

About this task

Installing a Guardium license key is a two-step process: you need to install the license key and then read and accept the terms of the license agreement. After installing a Guardium license key, the user interface will reload to reflect the functionality enabled by the new license.

Establishing a functional Guardium system requires installing both a base and at least one append licenses. The base license must be installed and accepted before installing and accepting any append licenses.

For more information about Guardium license keys, see [License keys](#).

Attention:

When upgrading a Guardium system, you will not need to apply licenses. License keys will be automatically generated based on your preexisting installation, but you will need to review and accept the license agreements before you can begin using your Guardium system. To review and accept licenses on an upgraded system, navigate to Setup > Tools and Views > License and click the Read and accept license link.

Procedure

1. Log in to your Guardium system as the `admin` user.
 2. Verify that the Machine Type displayed in the Guardium banner is correct for the system you are licensing.
The machine type will be one of the following:
 - Standalone
 - Central Manager
 - Aggregator
- Attention: If you are setting up a central manager and the Machine Type indicates an aggregator, convert the system from an aggregator to a central manager using the following CLI command: **store unit type manager**.
3. Install a base license.
 - a. Navigate to Setup > Tools and Views > License.
 - b. On the License page, enter the base key for your system in the License key field and click Apply to continue.
Attention: Depending on the system you are setting up, you will need to apply either a base collector key or a base aggregator key. A base aggregator key is required when setting up a central manager system.
 - c. From the License Agreement dialog, review the license agreement associated with the base key and click Accept when you are ready to accept the terms.
The Guardium interface will automatically refresh after accepting the agreement, but there will be no change in available functionality after installing a base license key.

4. Install one or more append licenses.

Repeat the following steps for each append licence you have purchased and want to install.

- a. Navigate to **Setup > Tools and Views > License**.
- b. On the License page, enter an append key in the License key field and click **Apply** to continue.
- c. From the License Agreement dialog, review the license agreement associated with the append key and click **Accept** when you are ready to accept the terms. The Guardium interface will automatically refresh after accepting the agreement, and any new functionality associated with the append license will become available.
- d. Repeat the steps in this section for each append license you want to install.

What to do next

In an environment with a central manager, you can distribute the new licenses by navigating to the **Manage > Central Management > Central Management** page and clicking the  icon to distribute licenses from the central manager to managed units.

In an environment with a central manager, the central manager and its managed units must use the same shared secret. Set the shared secret from the **Setup > Tools and Views > System** page or by using the CLI command **store system shared secret**.

License text is also available for download by starting the Guardium **fileserver** and navigating to `opt-ibm-guardium-log/install/[LICR number]`, where [LICR number] identifies the license you want to download.

Related concepts

- [License keys](#)

Related information

- [fileserver CLI command](#)

Install maintenance patches (if available)

You can install patches by using the CLI or through the GUI.

Note: In federated environments, maintenance patches can be applied to all of the appliances from the Central Manager.

There may not be any maintenance patches included with the installation materials. If any are included, follow these steps to apply them:

1. Log in to the Guardium® console, as the cli user, using the temporary cli password you defined in the previous installation procedure. You can do this by using an ssh client.

2. Do one of the following:

- If installing from a network location, enter the following command (selecting either ftp or scp):

```
store system patch install [ftp | scp]
```

And respond to the following prompts (be sure to supply the full path name to the patch file):

Host to import patch from:

User on <hostname>

Full path to patch, including name:

Password:

- If installing using the fileserver function, enter the following command:

```
store system install patch sys
```

You will be prompted to select the patch to apply. Use wildcards in the pathname to get multiple patches. Also separate patch names by commas.

3. To install additional patches, repeat step 2.

4. To see if patches have been installed successfully, use the CLI command:

```
show system patch installed
```

Patches are installed by a background process that may take a few minutes to complete.

Additional Steps (optional)

The following sections discuss changing the baseline English to another language, installing S-TAP® agents, defining Inspection Engines and installing CAS agents.

Change the language

Initial installation of Guardium® is always in English. Use the **store language** CLI command after installation to convert the database from English to the desired language. Setting the desired language is considered part of the initial system set up: changing the language on an established system will impact the information already captured, stored, customized, archived or exported on that system.

Important:

- After switching from English to a desired language, it is not possible to revert back to English using this CLI command. The Guardium system must be reinstalled in English.
- To prevent the system from displaying a mixture of languages, set a central manager and all its managed units to the same language.

Syntax

store language

Example

```
store language
The following languages are available on this appliance:
  1. French
  2. German
  3. Italian
  4. Japanese
  5. Korean
  6. Polish
  7. Pseudo
  8. Simplified Chinese
  9. Spanish
  10. Traditional Chinese
Please enter the number of the language you want or 0 to quit:
```

Install S-TAP agents

Install S-TAP agents on the database servers and define their inspection engines. S-TAP is a lightweight software agent installed on the database server, which monitors local and network database traffic and sends the relevant information to a Guardium system (the collector) for further analysis, reporting and alerting. To install an S-TAP, refer to the S-TAP section of this information center. To verify that the S-TAP have been installed and are connected to the Guardium system:

1. Log in to the administrator portal.
2. Do one of the following:

Navigate to the Manage > System View, and click S-TAP Status Monitor from the menu. All active S-TAPs display with a green background. A red background indicates that the S-TAP is not active.

Navigate to Manage > Activity Monitoring > S-TAP Control, and confirm that there is a green status light for this S-TAP.

Define Inspection Engines

Define Inspection Engines for network-based activity monitoring.

Install CAS agents

Install Configuration Auditing System (CAS) agents on the database server.

Creating the Virtual Image

Use this section to install the virtual image.

- [**VMware Infrastructure Overview**](#)
While you can install a Guardium VM on any VMware product, the VMware ESX server is the recommended platform for a virtual solution and is presented here.
- [**VM Installation Overview**](#)
To install the IBM Guardium VM, follow the steps that are described here. After you install the VM, return to earlier Step 3, Install the IBM Guardium image, and earlier Step 4, Initial Setup and Basic Configuration.
- [**Creating a Hyper-V Virtual Machine**](#)
- [**Red Hat Virtualization**](#)
Install Guardium in a Red Hat Virtualization environment.
- [**vMotion Installation**](#)
Guardium can be deployed in various virtualized environments, including a VMware virtual environment. In a vSphere deployment, this virtual environment includes the vMotion feature, which allows live migration of a virtual machine.

VMware Infrastructure Overview

While you can install a Guardium® VM on any VMware product, the VMware ESX server is the recommended platform for a virtual solution and is presented here.

The VMware ESX Server on which you can install the Guardium VM is one component of the VMware infrastructure. Although not all VMware Infrastructure components are required to support the Guardium VM, you should be familiar with all components that are in use at your installation.

ESX Server: This component is used to configure and control VMware virtual machines on a physical host referred to as the ESX Server host. To install an Guardium VM, you first define a virtual machine on an ESX Server host, and then install and configure the Guardium VM image on that virtual machine. You can create multiple Guardium VMs on a single ESX Server.

VI Client (Virtual Infrastructure Client): This component is used to connect to a standalone ESX Server, or to a VirtualCenter Server. In the latter case, you can administer multiple virtual machines created over multiple ESX Server hosts.

Web Browser: Use a Web browser to download and use the VI Client software from an ESX Server host or the VirtualCenter server.

VirtualCenter Management Server (Optional): This component runs on a remote Windows machine, and can be used to manage multiple virtual machines on multiple ESX Server hosts. It offers a single point of control over all the ESX Server hosts.

Database (Optional): The VirtualCenter Server uses a database to store configuration information for the infrastructure. The database is not needed if the VirtualCenter Server is not used.

License Server (Optional): Stores and manages the licenses needed to maintain a VMware Infrastructure.

For more information, go to www.vmware.com and search for “ESX Quick Start”

VM Installation Overview

To install the IBM® Guardium® VM, follow the steps that are described here. After you install the VM, return to earlier Step 3, Install the IBM Guardium image, and earlier Step 4, Initial Setup and Basic Configuration.

If you are installing multiple Guardium VM systems in a VMware VirtualCenter Management Server environment, you can create a template system from the first Guardium VM that you create, and then clone that template as necessary. Then, all you need to do is set the IP address on each cloned system. For more information, see the note following Step 7.

Step 1: Verify system compatibility

1. Verify that the host is compatible with VMware's ESX Server (ESX 4.0 Update 4 and higher is the bare minimum to run a Guardium system). See the VMware document entitled Systems Compatibility Guide for ESX Server, which is available online in PDF format.
2. Verify that a virtual machine installed on the host will be able to provide the minimum recommended resources for a Guardium system, whether you plan to use it as a collector, central manager, or aggregator. See the Minimum/Recommended Resources in the Hardware Requirements section of this document.
3. When you create a 64-bit VM for the first time or upgrade a 32-bit VM to 64-bit, ensure that the virtual hardware is correctly configured for 64-bit operation. In some cases, you might need to perform an Upgrade Virtual Hardware operation. For information, refer to your VMware documentation.

Step 2: Install VMware ESX Server

If it is not already installed, install VMware ESX Server. VMware provides installation instructions on their website to help with installing and configuring the VMware Infrastructure and ESX server.

Note: The ESX server is only supported on a specific set of hardware devices. For more information, see the VMware Virtual Infrastructure documentation.

Step 3: Connect network cables

Before you define any virtual switches that will be used for the Guardium VM, you must connect the appropriate NICs to the network. You cannot assign NICs to virtual networks or switches until the NICs are physically connected.

The following table describes how the Guardium VM uses network interfaces. Refer to this table to make the appropriate connections before you configure the virtual switches for use by the Guardium VM.

Table 1. IBM Guardium VM Network Interface Use

| Interface | Description |
|--|--|
| Proxy interface (the primary interface) | This interface is the main gateway to the appliance, and is used for these purposes: <ul style="list-style-type: none">• Graphical web-based User Interface (GUI) to manage, configure, and use the solution• Command Line Interface (CLI) for initial setup and basic configuration• Connections with external systems such backup systems, database servers, and LDAP server• Communication with other Guardium components such as other appliances (aggregator, central manager) and agents that are installed on database or file servers such as S-TAP® or CAS clients |
| Application server interface (the secondary interface) | This interface is required if you configure your Guardium system as a transparent proxy. It connects to the application servers whose content your Guardium system is configured to mask. |

Step 4: Configure the Guardium VM management portal

The default configuration for a new VMware ESX Server installation creates a single port group for use by the VMware service console and all virtual machines. For the Guardium VM, we strongly recommend that you do not share ports with the VMware console or any other virtual machine. Follow these instructions to create one or more virtual switches to be used by a Guardium VM.



1. Open the VMware VI Client, and log on to either a VirtualCenter Server, or the ESX Server host on which you want to create a new virtual machine.
2. If you are logged in to a VirtualCenter Server, click Inventory in the navigation bar, and expand the inventory as needed to display the managed host or cluster on which you plan to install a Guardium VM.
3. In the inventory display, click the host or cluster on which you plan to install a Guardium VM.
4. Click Configuration tab, click Networking in the Hardware box, and then click Add Networking.



This opens the Add Network Wizard, which is used for various purposes.

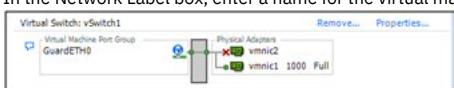
Use the Add Network Wizard to define a new virtual switch for the Guardium VM network interface. This is the connection over which you will access the Guardium VM management console, and over which the Guardium VM will communicate with other Guardium components (S-TAPs, for example, which are software agents that you will install later on one or more database servers).

5. In the Connection Types box, click Virtual Machine and click Next.
6. In the Network Access panel, click Create a virtual switch, and mark the unclaimed network adapter that you will use for the Guardium VM network interface.

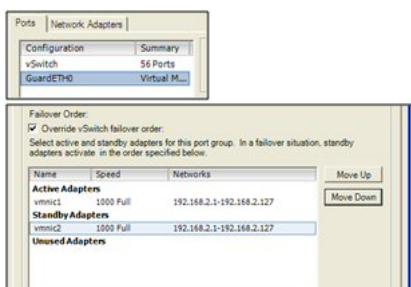


Note: The recommended network adapter type is VMXNET3. Avoid using the Flexible network adapter.

7. Optionally mark a second unclaimed network adapter if want to use the VMware IP teaming capability to provide a secondary (failover) network interface. Later, you will designate this second adapter as a Standby Adapter (and of course, you must cable both NICs appropriately).
8. Click Next to continue to the Connection Settings page of the Add Network Wizard.
9. In the Network Label box, enter a name for the virtual machine port group, for example: GuardETH0, and click Next.



10. In the Summary page, click Finish. The new virtual switch is displayed in the Configuration tab.
11. Optional. If you have defined a second adapter for failover purposes: (a) Click Properties link for the virtual switch just created to open the virtual switch Properties panel. (b) Click Ports tab and select the virtual port group just created (GuardETH0 in the example), and click Edit. (c) In the virtual port group Properties panel, click NIC Teaming tab, mark the Override vSwitch Failover box, and then move the second adapter to the Standby Adapters list. (d) Click OK to close the virtual port group Properties box, and click Close to close the virtual switch Properties box.



Step 5: Create a new virtual machine

If you have not already done so, create a new virtual machine on which to install a Guardium VM.

Perform this task by using the VMware VI Client.

1. Open the VMware VI Client, and log on to either a VirtualCenter Server, or the ESX Server host on which you want to create a new virtual machine.
2. If you are logged in to a VirtualCenter Server, click Inventory in the navigation bar, expand the inventory as needed, and select the managed host or cluster to which you want to add the new virtual machine.
3. From the File menu, click New – Virtual Machine to open the configuration Type panel of the New Virtual Machine wizard.
4. Click Typical as the configuration type, and click Next to continue with the Name and Folder panel.
5. On the Name and Folder panel:

Enter a name for the new virtual machine in the Virtual Machine Name field. This name appears in the VI Client inventory and is also used as the name of the virtual machines files.

To set the inventory location for the new virtual machine, select a folder or the root location of a datacenter from the list under Virtual Machine Inventory Location.

Click Next.

6. If your host or cluster contains resource pools, the Resource Pool panel is displayed, and you must select the resource (host, cluster, or resource pool) in which you want to run the virtual machine. Click Next.
7. On the Datastore panel, optionally select a datastore in which to store the new virtual machine files, and click Next.
8. In the Choose the Guest Operating System panel, choose the operating system that corresponds to the Guardium image that you are installing. Click Linux > RedHat Enterprise Linux 9, 64-bit from the Version box, and click Next.

The operating system is not installed now, but the OS type is needed to set appropriate default values for the virtual machine.

For VM minimum resources, refer to the Hardware Requirements in the Before you begin section.

9. On the Virtual CPUs panel, select the number of CPUs recommended for the type of Guardium VM being installed, and click Next.
10. On the Memory panel, select the amount of memory recommended for the type of Guardium VM being installed, and click Next. Important: the initial value must be at least 16 GB. If customers want to work outside the required range, consult with Technical Support.
11. On the Network panel, click 1 as the number of ports that are required, and click Next.

12. For the selected port, use the Network pull-down menu to choose a port group configured for virtual network use. (You should have defined this port group in the previous procedure.)
13. For the selected port group, mark the Connect at Power On check box (it should be marked by default), and click Next.
14. On the Virtual Disk Capacity panel, enter the amount of disk space to reserve for the new virtual machine in the Disk Size field.
15. On the Ready to Complete panel, verify your settings and click Finish.

This completes the definition of the new virtual machine. The operating system has not yet been installed, so if you attempt to start the virtual machine, that activity will fail.

Step 6: Install the Guardium system

Perform this task using the VMware Virtual Infrastructure Client.

1. Open the VMware VI Client, and log on to either a VirtualCenter Server, or the ESX Server host on which you want to create a new virtual machine.
2. If logged into a VirtualCenter Server, click Inventory in the navigation bar, expand the inventory as needed, and select the virtual machine on which you want to install the Guardium VM.
3. On the Summary tab, click Edit Settings.
4. Click CD/DVD Drive 1.
5. Select one of the following options to determine from where the virtual DVD device will read the Guardium Installation program. **We strongly recommend the first option:**

Datastore ISO File – Connect to the Guardium Installation ISO file on a datastore. If you have not already done so, copy the Guardium ISO files to a datastore accessible from the ESX Server host on which the virtual machine is installed. Click Browse to select the file.

Caution: For the remaining options, you will place the Guardium Installation DVD in a DVD drive. If you reboot any system with an Guardium Installation DVD in its DVD drive, you will install Guardium on that system, wiping out the host operating system and files.

Client Device – Connect to a DVD device on the system on which you are running the VI Client. If you select this option, insert the Guardium DVD in the DVD drive of the system on which the VI Client is running.

Host Device – Connect to a DVD device on the ESX Server host machine on which the virtual machine is installed. If you select this option, choose the device from a drop-down menu, and insert the Guardium DVD in the DVD drive of the ESX Server host machine.

6. Click OK.
7. Click Power On to start the virtual machine.
8. If you selected Client Device as your DVD Drive option, click Virtual CD-ROM (ide0:0) in the toolbar, and select the local DVD device to connect to.
9. Click Console tab to display the virtual machine console.
10. When asked if building a collector or aggregator, choose the appropriate type.

Caution: If a DVD drive was used, the DVD ejects when the installation completes. Be sure to remove the installation DVD from that drive. If the ISO file was used, be sure to remove the ISO CD ROM by changing the virtual CD/DVD back to a Client or Host Device. Otherwise, the next time it is rebooted, you will install Guardium on the host machine, wiping out the host machine operating system and all files.

The machine will reboot automatically, and you will be prompted to log in as the CLI user.

11. At this point, return to Step 4, Set up Initial and Basic Configurations for complete instructions on configuration of the Guardium system.

Step 7: Install Multiple VMs

(Optional) To install multiple GuardiumVMs, you can repeat the procedures for each appliance, or you can minimize your work by cloning the first Guardium VM that you created, and following these steps:

1. Use the VMware virtual infrastructure server product to clone the first Guardium VM that you configured to a template.
2. From the template, create a clone for each additional Guardium VM to be configured.
3. For each clone, log in to the Guardium VM console as the cli user by using the temporary cli password and reset any of the IP configuration parameters that you set in the previous procedure. Mandatory tasks: reset the IP address, reset the GLOBAL_ID (GID), and reset the host name. The UNIQUE_ID (UID) is set automatically and does not require manual configuration. Be sure to review all of the IP configuration settings entered in the previous procedure.

```
store network interface ip <ip_address>
store network interface mask <subnet_mask>
store product gid <n>
store system hostname <host_name>
```

When you are done, enter the **restart network** command.

```
restart network
```

Note: The unique ID (UID) of the appliance is recalculated every time the hostname changes in order to avoid having multiple appliances with the same unique ID.
Note: The global ID (GID) can be any number so long as it is unique and less than 9223372036854775808. During the cloning process this unique number is necessary. Please obtain the global IDs from your other appliances and use a number that is unique for this clone.

Creating a Hyper-V Virtual Machine

Before you begin

- Hyper-V is a virtualization solution from Microsoft. It is assumed that the Guardium user using Hyper-V has prior experience with Hyper-V.
- Verify system requirements for the version of Guardium® being installed.

Procedure

1. Start the Hyper-V Manager and connect to your Hyper-V server.

2. In the Actions pane, select **New > Virtual Machine** to begin the New Virtual Machine wizard. Click **Next**.
3. Specify names and location:
 - a. Name: This is the name of the virtual machine containing the Guardium system.
 - b. You may select Store the virtual machine in a different location and provide the path to your data store, if appropriate.
 - c. Click **Next** when done.
4. Specify Generation of the virtual machine: Select Generation 1 and click **Next**.
5. Assign memory: Verify that the allocated RAM meets the minimum system requirements. Leave the option **Use Dynamic Memory** for this virtual machine unchecked and click **Next**.
6. Configure Networking: Select your virtual switch and click **Next**. Note that hardware may differ and there may be multiple choices.
7. Connect Virtual Hard Disk: Select **Create a virtual hard disk**.
 - a. Specify the path to the virtual disk.
 - b. Verify that the size of the virtual hard disk meets the minimum system requirements.
 - c. Click **Next**.
8. Installation Options: The operating system can be installed through a physical CD/DVD drive or through an Image file (.ISO).
 - a. **DVD Installation:** select Physical CD/DVD drive and choose the correct drive letter.
 - b. **.ISO Installation:** select Image File (.ISO) and browse to your image file.
 - c. Click **Next**.
9. Complete installation: Verify all selected options in the Description box. Click **Finish** to create the virtual machine and close the wizard.
10. Open Console: Select your new virtual machine from the virtual machines pane and click **Connect**.
11. Click on **File > Settings**.
12. On the Hardware pane:
 - a. Select BIOS. Move IDE to the top of the Startup order.
 - b. Select the Processor section. Allocate the minimum number of virtual processors needed based on your system requirements.
 - c. Expand the Processor section. Select NUMA in the subsection and change the Maximum amount of memory (MB) to the assigned memory entered in the step 5.
 - d. Select the SCSI Controller section and click on the Remove button.
13. Optionally, in the Management pane below the Hardware pane, you may set up your preferences for Automatic Start up and Stop Actions.
14. Click **Apply** and if there are no warnings, click **OK**.
15. Click the green Start button to start your virtual machine.
16. Install your Guardium system. For more information see [Installing your Guardium Data Protection system](#). Power down after installation.
17. On the Hyper-v virtual machine console, open **File > Settings**.
18. On the Hardware pane, expand the Network Adapter section and select the Advanced Features subsection.
19. Configure the MAC address by selecting the Static radio button. Click **Apply** and **OK**.
20. Power on your virtual Guardium system.
21. 12.0 and later The installer automatically adds the necessary RPMs for Hyper-V.

Red Hat Virtualization

Install Guardium in a Red Hat Virtualization environment.

Before you begin

Red Hat Virtualization is a virtual machine platform based on Red Hat Enterprise Linux. This procedure assumes familiarity with the Red Hat Virtualization platform. For more information, see the Red Hat Virtualization documentation.

Procedure

1. Upload the Guardium ISO image on the system running the Red Hat Virtualization software using the following command:


```
engine-iso-uploader -i ISO
upload <Guardium ISO image
file name>.iso
```
2. Install the Virtual Viewer for your environment.

Access viewers at the following URL, then select and install the correct version for your environment: <https://<Red Hat Virtualization server host name>/ovirt-engine/rhv/client-resources>. For example, a 64-bit Windows users would select Virt Viewer for 64-bit Windows then Right-click > Install the virt-viewer-x64.msi file.
3. Log in to the Red Hat Virtualization server web interface: https://<Red Hat Virtualization server host name>/ovirt-engine/webadmin/?locale=en_US#dashboard-main
4. Open Compute > Virtual Machines and click **New** next to the Vms field to create a new virtual machine.
5. Configure the virtual machine as follows:
 - a. On the General page, define the following settings:
 - Operating System: Linux
 - Optimized for: High Performance
 - Name: provide a name for the virtual machine, for example gkvm04.
 - Description: provide a description for the virtual machine, for example Guardium 11.2.
 - nic1: 3148/3148
 - b. On the System page, define the following settings:
 - Maximum memory: 24576 MB
 - Total Virtual CPUs: 4
 - Configure the Hardware Clock Time Offset for your location.
 - c. On the Console page, clear the Headless Mode check box.
 - d. On the Boot Options page, define the following settings:
 - Second Device: CD-ROM
 - Check the Attach CD check box and select the Guardium ISO image.
 - Check the Enable menu to select boot device check box.
 - e. Click **OK** to save the settings.
6. From the Compute > Virtual Machines page, double-click the virtual machine created in the previous steps, select Disks and click **New** to create a new virtual disk.
7. From the New Virtual Disk page, select the Image page, define Size (GiB): 300, and click **OK**.

8. From the Compute > Virtual Machines page, click Run, and then click Console to open the remote console.
 9. From the console, press the **ESC** key to access the boot menu and select DVD/CD to boot the Guardium ISO image.
 10. From the Guardium Installer menu, select an installation type and install the Guardium system on the virtual machine.
-

vMotion Installation

Guardium can be deployed in various virtualized environments, including a VMware virtual environment. In a vSphere deployment, this virtual environment includes the vMotion feature, which allows live migration of a virtual machine.

vMotion is of two types, host and storage. Host vMotion is the live migration of the OS, and network transactions, from one hypervisor to another. Storage vMotion is the live migration of a running virtual machine's file system from one storage system to another. Both types of vMotion are supported by Guardium. For more information, see <https://www.vmware.com/products/vsphere/vmotion.html>.

Best Practices

- Configure your environment to support vMotion by using VMware documentation found here: <https://www.vmware.com/>. Contact VMware Support for configuration assistance.
- Guardium is a high performance, and high transaction system. Data is transferred between hypervisors in a host vMotion, and between storage systems in a storage vMotion. So, vMotion must be used when the Guardium appliance is shut down or at a low level of activity.
- The vMotion process is transparent to the virtual guest and does not affect the guest system. However, as part of a robust disaster recovery plan, verify that your backup and restore procedures are up to date.
- Guardium 11.4 and later includes **open-vm-tools**. If **open-vm-tools** is already installed, it is not necessary to install VMWare tools on the Guardium appliance.

VMWare Tools Installation

Install VMWare tools on the Guardium appliance by using these methods.

Method 1:

1. Open the VM client/console and select the VM instance that contains the InfoSphere Guardium appliance. Right-click the instance, select Guest > Install/upgrade VMware tools from the menu. Your instance is enabled to access the VMWare tools via a mount point.
2. To install VM tools, run the CLI command **setup vmware_tools install** from the VM client or console. For more information, see [setup vmware_tools install](#).

Method 2:

1. Open the VMware VI Client, and log on to either a VirtualCenter Server, or the ESX Server host on which you want to upgrade the VMware Tools.
2. If you are logged in to a VirtualCenter Server, click inventory in the navigation bar, expand the inventory as needed, and select the virtual machine on which you want to upgrade VMWare Tools.
3. On the Summary tab, click Edit Settings and select CD/DVD Drive 1.
4. The virtual CD-ROM/DVD device reads the VMware Tools program from the datastore ISO File. To enable this device, click Browse and select the VMware Tools ISO file on a datastore. If you have not already done so, copy the VMware Tools ISO file to a datastore accessible from the ESX Server host on which the virtual machine is installed.

Note: The file name for the VMware Tools package must not be modified when the ISO image is created.

5. To create the ISO, run the appropriate command. This command can differ based on the OS running on your system.

Example of a LINUX command:

```
mkisofs -r -J -L -l -allow-lowercase -allow-multidot -N -v -d -o vmware_tools3.iso vmware_tools/
```

Check the Mkisofs documentation for more information.

6. Under Device status check the Connected checkbox. Click OK.
7. From the VM Console screen, log in using CLI.
8. Run the CLI command **setup vmware_tools install** and press the Enter key on your keyboard. For more information, see [setup vmware_tools install](#)
9. When the installation is complete, you are brought back to the CLI prompt. Disconnect the CD/DVD drive from the ISO on the datastore.

open-vm-tools updates

For Guardium 12.0 and later, **open-vm-tools** is up to date with the latest 9.X Extended Update Support (EUS) stream.

Custom Partitioning

If you customize the partitioning of the hard drive, you must make several choices.

1. Choose Custom Partitioning Installation from the boot screen.

Choose Create custom layout and use the recommended partitioning scheme listed here.

Note: The boot loader, a special program that loads the operating system into memory, is part of any custom partitioning installation.

2. Create custom layout. In this case, there are existing partitions on the disk. Do not delete any partitions. Choose the custom layout selection to add whatever partitions you want to what is already on the disk. The following table specifies recommended values for custom layout.

Table 1. Recommended values for custom layout

| Partitions | Values |
|--------------|------------------|
| / | 25 GB |
| Swap portion | half of RAM size |
| /boot | 5 GB |
| /var | All the rest |

All the available drives are also displayed on this screen. Choose the drive for the partitioning and then installation.

After the partitioning is finished, the Guardium® system software is installed automatically.

If values are created that exceed the space available on the disk, an error message appears.

Click OK to reboot the system and return to the beginning of Custom Partitioning.

See the Red Hat Enterprise Linux documentation for more information about how the Red Hat distribution handles partitioning.

Note: Non-default partitioned systems - Custom partitioned systems cannot be upgraded using an upgrade patch. Instead, you must use the backup, rebuild, and restore method. If there is uncertainty regarding the partitioning of systems, download and install Health Check p9997. The resulting patch log contains information regarding system partitioning.

How to partition with an encrypted LVM

If you use an encrypted disk, create an encrypted LVM volume that contains the / and /var logical volumes.

About this task

The following procedure requires either physical or remote console access to the Guardium system.

Procedure

1. Insert the IBM® Guardium® DVD and boot the machine.
2. Choose Custom Partition Installation from the boot screen.
3. Press Enter.
4. In the Installation Summary, select Installation Destination. Under Other Storage Options, select I will configure partitioning and check Encrypt my data.
5. Select Click here to create them automatically and change the Mount Point and Name from home to var. Click Done.
6. When prompted, enter a Disk encryption passphrase and safeguard it. Click Save Passphrase and Accept Changes.
Tip: The encryption passphrase is required to unlock the LVM volume when you restart the system. This key cannot be replaced if lost.
7. Optional: You can set up a tang server to automatically enter the encryption key and unlock each volume of your encrypted disks when you restart your system. If a tang server is down when rebooting, the message dracut-initqueue: Error communicating with server appears. You must then unlock the encrypted machine by manually entering the passphrase.
Tip: Set up the tang server by using the CLI command **store tang server** or by using the API command **grdapiclevis_bind** on your central manager to bind all your managed units to a tang server. For more information on the commands, see [store tang server](#), [reset luks keys](#), and [grdapiclevis_bind](#).

Related reference

- [grdapiclevis_bind](#)

Related information

- [store tang server](#)
- [reset luks keys](#)

Create an LVM disk with four disks

About this task

Use the following instructions to create an IBM Guardium VM with 4 Hard disks, LSI Logic Parallel SCSI controller, and E1000 network adapter.

Procedure

1. Click on Edit Settings of the Guardium VM appliance.
2. Mount a Guardium V10.6 ISO image. Make sure the following items are selected:
 - Connected
 - Connect at Power On
3. Click VM Options > Boot Options. Select the During the boot, force entry into the BIOS setup screen check box, and click OK.
4. Power on the Guardium VM.

5. In the setup screen, select Boot from the menu, and click CD-ROM Drive, and move it to the top.
 6. From the menu, select Exit . Click Exit Saving Changes and press the Enter key.
 7. Select Yes to save configuration changes, and exit. This will start the installation.
 8. In the IBM InfoSphere Guardium Installer, select Custom Partition installation (Graphical Mode).
 9. In the Storage Device Warning dialog, click on Yes, discard any data.
 10. To configure the installation type, select the Use All Space radio button. Then, select the Review and modify partitioning layout check box, and click Next.
 11. Under Data Storage Devices, select all four VMware virtual disks, and then click the right arrow.
 12. Under Install Target Devices, select the first disk for Boot loader, and click Next.
 13. Under LVM Volume groups, select lv_home and click Edit.
 14. In the Edit Logical Volume dialog, click the drop down for Mount Point, and select /var. In the Logical Volume Name text box, enter lv_var. Click ok.
 15. In the Format warnings dialog, click Format.
 16. To start installation, select Install boot loader on /dev/sda and click Next.
- Note: The Guardium VM will reboot when the installation complete.
-

Example of SAN Configuration

This appendix details the steps involved in moving to a command prompt in order to pre-partition a hard drive (as is needed for SAN installation).

First partition space on the SAN storage device, and then install the IBM® Guardium® OS. Choose one hard disk for this installation.

Note: Depending on what SAN hardware is used, specific instructions may be different. Installation on a SAN is supported; installation on a NAS is not supported.

Summary of steps

1. Enter system setup (press F1 on IBM servers during initial boot) and modify the Start Options to select the appropriate PCI slot to boot from (where the QLogic Card is).
2. Modify the BIOS for the QLogic card by pressing Ctrl-Q, when the QLogic BIOS is loading, to enable it to be a boot device. Then select the LUN (logical unit number) of the boot device.
3. Boot from the RedHat 5.8 DVD and enter Rescue mode in order to run fdisk and create partitions on the SAN device using the specifications listed here:

Table 1. Partitions on SAN device

| Partitions | Space |
|------------|--------------------------------|
| 1 | 500 MB for /boot |
| 2 | Amount of system memory + 4 GB |
| 3 | 25 GB for / |
| 4 | All remaining space for /var |

Note: While the RedHat installation process would allow you to create the partitions and load the OS, the system does not boot properly after the installation unless the partitions are pre-created with **fdisk**.

4. Proceed with the OS installation utilizing the previously defined partitions (use only the /dev/sda device).
5. Reboot and finish the remaining installation steps (hostname, IP configuration, and so on).

Note:

In the SAN environment, the single LUN is presented to RedHat 5.8 as multiple devices due to redundant paths within the network switch(es) on the SAN. (The SDD storage was eight devices.)

This is a function of the SAN storage brand/type and how it is configured at each site.

It is very important to only edit the existing partitions that the IBM Guardium installation sees by adding the mount point and setting the file system (ext4 or swap,) and not changing other settings (such as size) and to unselect all devices other than /dev/sda when selecting which device to load the OS on.

Instructions for running fdisk

Follow these instructions for running **fdisk** to pre-partition the SAN storage from RedHat rescue mode:

1. Assuming SAN is the only storage attached to the server, type **fdisk /dev/sda**. Type **y** if a warning appears regarding working on the whole device.
2. Type **n** for a new partition.
3. Type **p** for a primary partition.
4. Type **1** for partition #1.
5. Press Enter to accept the default start location.
6. Type **+512M** to make partition 1 500MB in size (this will be the /boot partition).
7. Type **n** for a new partition.
8. Type **p** for a primary partition.
9. Type **2** for partition #2.
10. Press Enter to accept the default start location.
11. Type **+12288M** to make partition 2 12GB in size (this assumes 8GB of physical RAM). The recommended size is physical RAM + 4GB (this will be the swap partition).
12. Type **n** for a new partition.
13. Type **p** for a primary partition.
14. Type **3** for partition #3.
15. Press Enter to accept the default start location.
16. Type **+10240M** to make partition 3 10 GB in size (this will be the / partition).
17. Type **n** for a new partition.
18. Type **p** for a primary partition (will default to partition #4).
19. Press Enter to accept the default start location.
20. Press Enter to fill to maximum size (this will be the /var partition).
21. Type **w** to write the partition table to the SAN.
22. Type **exit** to exit rescue mode and reboot to begin the Custom Partition Installation (Step 3, Install the IBM Guardium image).

Examples of screenshots for QLogic setup

The Q-Logic screens used here are representative of the steps needed. Other Fiber Channel cards can be used.

1. Modify the BIOS for the QLogic card by pressing CTRL-D. This is the first screen presented after pressing Ctrl-Q when prompted to enter the Configuration Setup Utility. This is a two-port card; select the appropriate port and press Enter.



2. Press Enter to change Configuration Settings.



3. Press Enter to change Adapter Settings.



4. Use your arrow keys to select Host Adapter BIOS and press Enter to toggle to Enabled.



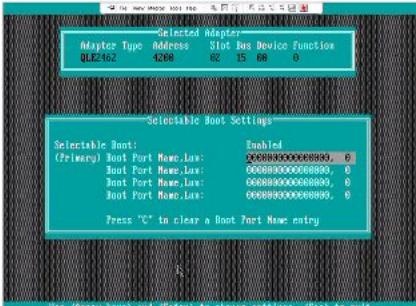
5. Press Esc to back up to the previous screen and use the down-arrow to select Selectable Boot Settings and press Enter.



6. Press Enter to change Selectable Boot to Enabled.



7. Select the first Boot Port Name, LUN and press Enter to display a list of LUNs. If you are configuring the proper card/port, the LUN number(s) appear here. Select the first one in the list.



8. Press Esc until you have backed out to the screen that says Reboot and select it to reboot the system. You are now ready to proceed with the IBM Guardium installation.

Upgrading your Guardium system

Upgrade your IBM® Guardium® system to the latest offering.

- [Planning an upgrade](#)
Review upgrade scenarios and identify the correct upgrade path for your Guardium systems.
- [Upgrading an environment with a central manager](#)
Upgrade your central manager environment to the next major version.
- [Upgrading a stand-alone system](#)
Upgrade your stand-alone system to the next major version.

Planning an upgrade

Review upgrade scenarios and identify the correct upgrade path for your Guardium® systems.

- [Identifying the correct upgrade path](#)
The best approach for upgrading IBM Guardium depends on the version you are upgrading from, the hardware of your system, and any special partitioning requirements you might have.
- [Mixed-version environments during an upgrade](#)
During an upgrade, your Guardium environment enters a mixed-version state with restricted functionality.
- [Upgrading with central managers and aggregators](#)
Minimize disruptions to your Guardium environment by following a top-down upgrade approach.

Identifying the correct upgrade path

The best approach for upgrading IBM Guardium® depends on the version you are upgrading from, the hardware of your system, and any special partitioning requirements you might have.

Before you begin

Before you upgrade to Guardium 12.x, take the following actions:

- Disable TLS 1.0 and TLS 1.1 in your environment. Guardium 12.0 requires TLS 1.2 or later, and any managed units or S-TAPs that do not support at least TLS 1.2 are disconnected after upgrade. From a central manager, use an API command `grdap1 disable_deprecated_protocols all=true` to identify any connected components that do not support at least TLS 1.2. Upgrade those components to TLS 1.2 or later so they remain connected after the upgrade. For more information, see [Managing the TLS version](#).
- Configure a system backup with secure file copy (SCP) or secure file transfer protocol (SFTP) on all Guardium systems to upgrade, even if a system backup was never configured for those systems. The upgrade patch creates and sends an upgrade backup file to a remote server by using the current appliance system backup configuration to determine the destination for that file.

About this task

Determine the current Guardium version and patch level by clicking the Help icon in the product and selecting About Guardium. The following table describes how to upgrade to the latest Guardium version.

| Current Guardium version | Upgrade path |
|--------------------------|--|
| Version 11.5 | 1. Archive and purge system data.
2. Backup your system. Include both your data and configuration files.
3. Apply health check patch 11.0p9998.
4. Apply the latest version 12 upgrade patch.
5. 12.1 and later Apply health check patch 12.0p9997.
6. 12.1 and later Apply the latest version 12 GPU and maintenance patches, if available. |
| Versions 11.0 to 11.4 | 1. Apply health check patch 11.0p9997.
2. Archive and purge system data.
3. Backup your system. Include both your data and configuration files.
4. Apply the version 11.5 GPU and maintenance patches.
5. Follow the version 11.5 upgrade path that is described in the Procedure . |
| Version 10.6 | 1. Apply health check patch 10.0p9998.
2. Archive and purge system data.
3. Backup your system. Include both your data and configuration files.
4. Apply the latest version 11 upgrade patch.
5. Apply health check patch 11.0p9997.
6. Apply the latest version 11 GPU and maintenance patches (to get to version 11.5).
7. Follow the version 11.5 upgrade path that is described in the Procedure . |

The version 12 upgrade patch is incompatible with the following configurations:

- Guardium systems with custom partitions.
- Encrypted Logical Volume Management (LVM) disks.
- Guardium systems that are deployed in cloud environments.

If your upgrade scenario satisfies the following conditions, use the procedure that is described in the following technote to upgrade your environment:
<https://www.ibm.com/support/pages/node/7032147>.

1. You are upgrading an environment with a central manager.
2. You are upgrading from versions 10.6, 11.0, or 11.1 to versions 11.5, 12.0 or later.

Procedure

1. Apply the latest health check patch that is relevant to your version.
 - For version 12.0 and later, apply health check patch 12.0p9997.
 - For version 11.5 or earlier, apply health check patch 11.0p9998.
 - For version 10.6, apply health check patch 10.0p9998.
2. Archive and purge system data.
3. Backup your system including your data and configuration files.
4. Rebuild the appliance by using the latest version 12 ISO.
5. Apply the latest version 12 GPU.
6. Apply the relevant maintenance bundle, sniffer, and security patches.
Important: If you applied the maintenance patches a few weeks earlier, apply the version 12 health check patch (12.0p9997) to confirm that the system is ready before you continue to the next step.
7. Restore the system backup. Include both your data and configuration files.

What to do next

After you upgrade to Guardium 12.x, take the following actions:

- To restore backups that are taken before the upgrade to 12.0, disable FIPS mode, restore the backups, and then re-enable FIPS mode.
Important: To run configuration auditing system (CAS) with FIPS mode enabled, the CAS server requires TLS 1.2 to be enabled and the CAS client requires IBM Java 8 SR7 or later.
- After you upgrade to 12.0 or later, custom SHA256 GIM certificates are required before you can deploy new SHA256-signed GIM bundles. For more information, see [Updating Guardium Data Protection GIM clients with SHA256 certificates](#).
- If you use S-TAP for z/OS with TLS 1.3, verify that the z/OS version is 2.04 or later.
- 12.0 After you upgrade from 11.x to 12.0, you can log in to the CLI only after you change the password.

Mixed-version environments during an upgrade

During an upgrade, your Guardium® environment enters a mixed-version state with restricted functionality.

Guardium upgrades cannot be completed on all systems (central managers, aggregators, and collectors) and all S-TAPs simultaneously. As a result, your environment enters a mixed-version state during the upgrade process. For example, after upgrading a central manager to the latest version, managed units continue operating at the previous version level until they are also upgraded.

Although mixed-version environments are supported, several limitations exist. For example, while data collection, data assessment, and policies (with some restrictions) continue working in a mixed-version environment, some new or enhanced functionality is not available until all systems are upgraded.

Important: Upgrade your entire environment to the latest release and patch level as soon as possible.
Be aware of the following restrictions while operating in a mixed-version environment:

- Complete functionality is not available until the entire environment has been upgraded to the latest release and patch level.
- Do not make configuration changes while operating in a mixed-version environment.
- Disable TLS 1.0 and TLS 1.1 in your environment. Guardium 12.0 requires TLS 1.2 or later, and any managed units or S-TAPs that do not support at least TLS 1.2 are disconnected after upgrade. From a central manager, use an API command `grdapi disable_deprecated_protocols all=true` to identify any connected components that do not support at least TLS 1.2. Upgrade those components to TLS 1.2 or later so they remain connected after the upgrade. For more information, see [Managing the TLS version](#).
- After you upgrade to 12.0 or later, custom SHA256 GIM certificates are required before you can deploy new SHA256-signed GIM bundles. For more information, see [Updating Guardium Data Protection GIM clients with SHA256 certificates](#).
- Central managers on version 11.5 do not support registration of new managed units that are lower than version 11.5.

Upgrading with central managers and aggregators

Minimize disruptions to your Guardium® environment by following a top-down upgrade approach.

This means first upgrading one high-level system and then upgrading the systems or agents that report to it, then upgrading the next high-level system and the systems or agents that report to it, and so on. This approach minimizes the impact of operating a mixed-version Guardium environment.

A top-down approach is necessary because an upgraded aggregator can aggregate data from older releases, but an older aggregator cannot aggregate data from collectors on newer releases. Similarly, an upgraded central manager can manage units running older releases, but the managed units are not fully functional until they are upgraded to match the central manager.

To avoid these issues, upgrade a central manager before upgrading any of its managed units. If you have multiple central managers, first upgrade one central manager and then upgrade its managed units before going on to upgrade the next central manager and its managed units.

Similarly, upgrade an aggregator before upgrading any units that export data to it. If you have several aggregators, first upgrade one aggregator and then upgrade the collectors that report to it before going on to upgrade the next aggregator and its collectors.

Finally, upgrade a collector before upgrading the S-TAPs registered to it. Upgrade one collector and all the S-TAPs registered to it before going on to upgrade the next collector and its S-TAPs.

Use failover collectors to ensure that the data collection from S-TAPs is not interrupted during the upgrade process.

This is the most efficient approach for establishing compatible systems in each branch of your environment.

Upgrading an environment with a central manager

Upgrade your central manager environment to the next major version.

1. [Preparing for upgrade in a managed environment](#)

The upgrade patch promotes your Guardium system to the next major version. In an environment with a central manager, you must first upgrade your central manager and then the managed units. Use the following workflow to prepare your central manager and managed units for upgrade.

2. [Upgrading the central manager](#)

Upgrade your central manager to the next major version.

3. [Upgrading the managed unit](#)

Upgrade your managed units after upgrading your central manager.

4. [Upgrading S-TAP agents in a managed environment](#)

After you upgrade your central manager and managed units, upgrade your S-TAP agent.

Preparing for upgrade in a managed environment

The upgrade patch promotes your Guardium® system to the next major version. In an environment with a central manager, you must first upgrade your central manager and then the managed units. Use the following workflow to prepare your central manager and managed units for upgrade.

Procedure

1. Ensure that you meet the minimum system requirements. For more information, see [Hardware requirements](#).
2. Plan your upgrade strategy. For more information, see [Planning an upgrade](#).
3. Identify your upgrade path and download the relevant patches from the IBM Fix Central website. For more information, see [Identifying the correct upgrade path](#).
 - The latest applicable health check patch.
 - The latest upgrade patch or GPU.
 - All applicable maintenance patches, such as the latest bundle, security fix, and sniffer patch. To view the list of available patches, access the home page of the Guardium UI and click the bell icon.
 - Base and append licenses.
4. Upgrade your firmware to the most recent version provided by your vendor. If you use a Guardium appliance, check the Fix Central website for the latest firmware.
5. If you want to use an external storage system for your archive and backup, ensure that you have the configuration details ready. For more information, see [Configuring external storage](#).
6. Unmount all media such as DVDs or USB disks that are mounted either directly or virtually on the physical appliance. Mounted media might cause the upgrade to fail.
7. Schedule the installation during a quiet time on your Guardium system to avoid conflicts with other long-running processes such as heavy reports, audit processes, backups, and imports.

8. Set the time to the local time zone and synchronize time across all your Guardium systems and agents by using a Network Time Protocol (NTP) server.

Next topic: [Upgrading the central manager](#)

Related information

- [Understanding Guardium patch types and patch names](#)
-

Upgrading the central manager

Upgrade your central manager to the next major version.

1. Applying the health check patch on central managers

The health check patch performs preliminary checks on your Guardium system to prevent potential issues during the upgrade. This patch must be successfully installed on your central manager in the last seven days before you install the Guardium upgrade patch.

2. Archiving data from central managers

You can archive the audit data that is captured by your Guardium system to another location. These archived files can be restored later for forensic purposes without replacing the audit data that is already available in your Guardium system. Use the following procedure to archive data on your central manager.

3. Purging system data from central managers

Purging unnecessary data from the Guardium system can significantly speed up the upgrade process. For best performance and to minimize risks that are associated with upgrading large amounts of data, try to achieve less than 20% internal database utilization by purging unnecessary system data. Use the following procedure to purge data from your central manager.

4. Backing up a central manager

System backups store all the necessary data and configuration values to restore your Guardium system. Use the following procedure to back up your central manager.

5. Applying the upgrade patch on central managers

To upgrade your central manager, you must install the upgrade patch. You can install the patch from your local system, from a network location, from a file server, or by using media such as a CD or DVD.

6. Installing maintenance patches on central managers

After you upgrade your central manager, apply the relevant maintenance patches.

Previous topic: [Preparing for upgrade in a managed environment](#)

Next topic: [Upgrading the managed unit](#)

Applying the health check patch on central managers

The health check patch performs preliminary checks on your Guardium® system to prevent potential issues during the upgrade. This patch must be successfully installed on your central manager in the last seven days before you install the Guardium upgrade patch.

Procedure

1. Install the patch by using the CLI command **store system patch install**. For more information, see [store system patch install](#).
2. When prompted, select the health check patch from the list of available patches.
3. Monitor the installation by using the CLI command **show system patch installed**.

If the health check patch is an incorrect version, the installation fails with the error message Patch Installation Failed - Latest patch *patch_version_number* required.

Next topic: [Archiving data from central managers](#)

Related concepts

- [System CLI commands](#)
-

Archiving data from central managers

You can archive the audit data that is captured by your Guardium® system to another location. These archived files can be restored later for forensic purposes without replacing the audit data that is already available in your Guardium system. Use the following procedure to archive data on your central manager.

Procedure

1. Go to Manage > Data Management > Data Archive.
2. Select the Archive checkbox.
3. In the Archive data older than field, enter a value and select a unit of time from the menu.
For example, to archive data from yesterday, enter the value 1, and select Day(s) from the menu.
Tip: If you archive data on a schedule, check your archive log by accessing Manage > Reports > Data Management > Aggregation/Archive Log to ensure that there are no data gaps in your archive.
4. In the Ignore data older than field, enter the time interval to archive.
For example, to archive one day's data, enter 2. Any value that is specified here must be greater than the Archive data older than value. If you leave this field blank, you archive data for **all days** older than the value specified in Archive data older than.

5. Select the Archive Values checkbox to include values from SQL strings in the archived data. If this option is not selected, the values are replaced with question mark characters and are not available after the restore operation.
6. Select the Protocol that you want to use to store your archive and enter the configuration details.
7. Click Test connection The system verifies the configuration by sending a test data file to the configured location. If the operation fails, an error message is displayed.
8. Click Save to save the configuration changes. If the operation fails, an error message is displayed and the configuration is not saved.
9. Click Run Once Now to run the operation now.

What to do next

Go to [Manage > Reports > Data Management > Aggregation/Archive Log](#) to verify that the archive operation is successful. Each archive operation shows multiple activities. Ensure that the status of each activity is Succeeded.

Previous topic: [Applying the health check patch on central managers](#)

Next topic: [Purging system data from central managers](#)

Related concepts

- [File Handling CLI Commands](#)

Related tasks

- [Configure data archive](#)
- [Configuring external storage](#)

Purging system data from central managers

Purging unnecessary data from the Guardium® system can significantly speed up the upgrade process. For best performance and to minimize risks that are associated with upgrading large amounts of data, try to achieve less than 20% internal database utilization by purging unnecessary system data. Use the following procedure to purge data from your central manager.

Procedure

1. Open [Manage > Data Management > Data Archive](#).
2. Click the Purge checkbox to define a purge operation.
Important: Changes made to the Data Archive purge configuration is also applied to the Data Export purge configuration.
3. Define a Purge data older than time period.
All data older than the specified period of days, weeks, or months are purged from the system.
4. Click the Allow purge without archiving or exporting checkbox.
5. Click Save to save the configuration changes.
6. Click Run Once Now to run the purge operation and purge old system data.

What to do next

Open [Manage > Reports > Activity Monitoring > Scheduled Jobs](#) to monitor the status of the data archive job.

Previous topic: [Archiving data from central managers](#)

Next topic: [Backing up a central manager](#)

Backing up a central manager

System backups store all the necessary data and configuration values to restore your Guardium® system. Use the following procedure to back up your central manager.

Before you begin

Determine whether you have sufficient disk space available for backup.

Tip:

For a successful backup, ensure that the DB utilization size < available disk space for backup.

You can use the following formula to calculate the disk space available for backup:

Available disk space for backup = free space available in your /var partition - 10% of the total size of your /var partition.

To find the disk size of your /var partition, navigate to [Manage > System View > System Monitor](#). On the Hard Disk Usage tile, click Tabular View to list the values for the total disk size, free disk space, and used disk space for your partitions.

Procedure

1. Go to [Manage > Data Management > System Backup](#).
2. Select the Protocol that you want to use for your backup and enter the configuration details.
3. Select one or both of the backup options:
 - Select Configuration to back up important definitions.

- Select Data to back up all data.
- Backing up both configuration and data is recommended for most deployments. In deployments where the data is not needed, for example if the data collected by Guardium is sent to another system for processing, backing up only the configuration and excluding the data is faster and produces a smaller backup file.
- Warning: If data is not backed up, it cannot be restored later.
4. Click Save to verify and save the configuration changes. The system verifies the configuration by sending a test data file to your chosen location for backup. If the operation fails, the configuration is not saved and an error message is displayed.
 5. Click Run Once Now to run the operation once.

What to do next

Go to Manage > Reports > Data Management > Aggregation/Archive Log. Verify that the operation has Succeeded.

Previous topic: [Purging system data from central managers](#)

Next topic: [Applying the upgrade patch on central managers](#)

Related tasks

- [Configuring external storage](#)

Related information

- [store storage-system](#)

Applying the upgrade patch on central managers

To upgrade your central manager, you must install the upgrade patch. You can install the patch from your local system, from a network location, from a file server, or by using media such as a CD or DVD.

About this task

The installation time depends on the amount of data that is involved, your system's specifications, and configurations. After the patch installation completes, the upgrade process begins automatically and the system restarts. Do not restart the system manually.

After restart, the system begins the following processes:

- Network configuration, database data migration, database startup.
- License upgrade and language setting.
- Database restart, certificate and key migration, password migration, and file clean-up.

Procedure

1. Install the patch by using the CLI command **store system patch install**. For more information, see [store system patch install](#).
2. When prompted, select the upgrade patch from the list of available patches.
3. Monitor the installation by using the CLI command **show system patch installed**. After installation is complete, the system restarts automatically.

Previous topic: [Backing up a central manager](#)

Next topic: [Installing maintenance patches on central managers](#)

Installing maintenance patches on central managers

After you upgrade your central manager, apply the relevant maintenance patches.

Procedure

1. Install the patch by using the CLI command **store system patch install**. For more information, see [store system patch install](#).
2. Select the maintenance patch to install.

What to do next

Repeat the procedure to install all the relevant maintenance patches.

Previous topic: [Applying the upgrade patch on central managers](#)

Related information

- [Understanding Guardium patch types and patch names](#)

Upgrading the managed unit

Upgrade your managed units after upgrading your central manager.

1. [Applying the health check patch on managed units](#)

The health check patch performs preliminary checks on your Guardium® system to prevent potential issues during the upgrade. This patch must be successfully installed in the last seven days before you install the Guardium upgrade patch. Use the following procedure to distribute the health check patch to your managed units by using the Central Management page on the central manager.

2. [Archiving data from managed units](#)

You can archive the audit data that is captured by your Guardium system to another location. These archived files can be restored later for forensic purposes without replacing the audit data that is already available in your Guardium system. Use the following procedure to archive the data on your managed unit.

3. [Purging system data from managed units](#)

Purging unnecessary data from your managed unit can significantly speed up the upgrade process. For best performance and to minimize risks that are associated with upgrading large amounts of data, try to achieve less than 20% internal database utilization by purging unnecessary system data.

4. [Backing up a managed unit](#)

System backups store all the necessary data and configuration values to restore your Guardium system. Use the following procedure to back up a managed unit in your centrally managed environment.

5. [Applying the upgrade patch on managed units](#)

Upgrade your managed unit by distributing the upgrade patch from the central manager. Upgrade the aggregators first before you upgrade collectors.

6. [Installing maintenance patches on managed units](#)

Distribute the maintenance patches to your managed units by using the Central Management page on the central manager.

Previous topic: [Upgrading the central manager](#)

Next topic: [Upgrading S-TAP agents in a managed environment](#)

Applying the health check patch on managed units

The health check patch performs preliminary checks on your Guardium® system to prevent potential issues during the upgrade. This patch must be successfully installed in the last seven days before you install the Guardium upgrade patch. Use the following procedure to distribute the health check patch to your managed units by using the Central Management page on the central manager.

Before you begin

Ensure that the most recent health check patch for upgrades is installed on your central manager.

Procedure

1. On your central manager, go to Manage > Central Management > Central Management
2. Select your managed units and click Patch Distribution.
3. Select the patch to distribute and click Install Patch Now to install the patch immediately. To schedule the installation later, click Schedule Patch.

Next topic: [Archiving data from managed units](#)

Archiving data from managed units

You can archive the audit data that is captured by your Guardium® system to another location. These archived files can be restored later for forensic purposes without replacing the audit data that is already available in your Guardium system. Use the following procedure to archive the data on your managed unit.

Procedure

1. Go to Manage > Data Management > Data Archive.
2. Select the Archive checkbox.
3. In the Archive data older than field, enter a value and select a unit of time from the menu.
For example, to archive data from yesterday, enter the value 1, and select Day(s) from the menu.
Tip: If you archive data on a schedule, check your archive log by accessing Manage > Reports > Data Management > Aggregation/Archive Log to ensure that there are no data gaps in your archive.
4. In the Ignore data older than field, enter the time interval to archive.
For example, to archive one day's data, enter 2. Any value that is specified here must be greater than the Archive data older than value. If you leave this field blank, you archive data for **all days** older than the value specified in Archive data older than.
5. Select the Archive Values checkbox to include values from SQL strings in the archived data. If this option is not selected, the values are replaced with question mark characters and are not available after the restore operation.
6. Select the Protocol that you want to use to store your archive and enter the configuration details.
7. Click Test connection The system verifies the configuration by sending a test data file to the configured location. If the operation fails, an error message is displayed.
8. Click Save to save the configuration changes. If the operation fails, an error message is displayed and the configuration is not saved.
9. Click Run Once Now to run the operation now.

What to do next

- Go to Manage > Reports > Data Management > Aggregation/Archive Log to verify that the archive operation is successful. Each archive operation shows multiple activities. Ensure that the status of each activity is **Succeeded**.

Previous topic: [Applying the health check patch on managed units](#)

Next topic: [Purging system data from managed units](#)

Purging system data from managed units

Purging unnecessary data from your managed unit can significantly speed up the upgrade process. For best performance and to minimize risks that are associated with upgrading large amounts of data, try to achieve less than 20% internal database utilization by purging unnecessary system data.

Procedure

1. Open Manage > Data Management > Data Archive.
2. Click the Purge checkbox to define a purge operation.
Important: Changes made to the Data Archive purge configuration is also applied to the Data Export purge configuration.
3. Define a Purge data older than time period.
All data older than the specified period of days, weeks, or months are purged from the system.
4. Click the Allow purge without archiving or exporting checkbox.
5. Click Save to save the configuration changes.
6. Click Run Once Now to run the purge operation and purge old system data.

What to do next

- Open Manage > Reports > Activity Monitoring > Scheduled Jobs to monitor the status of the data archive job.

Previous topic: [Archiving data from managed units](#)

Next topic: [Backing up a managed unit](#)

Backing up a managed unit

System backups store all the necessary data and configuration values to restore your Guardium® system. Use the following procedure to back up a managed unit in your centrally managed environment.

Before you begin

Determine whether you have sufficient disk space available for backup.

Tip:

For a successful backup, ensure that the DB utilization size < available disk space for backup.

You can use the following formula to calculate the disk space available for backup:

Available disk space for backup = free space available in your /var partition - 10% of the total size of your /var partition.

To find the disk size of your /var partition, navigate to Manage > System View > System Monitor. On the Hard Disk Usage tile, click Tabular View to list the values for the total disk size, free disk space, and used disk space for your partitions.

Procedure

1. Go to Manage > Data Management > System Backup.
 2. Select the Protocol that you want to use for your backup and enter the configuration details.
 3. Select one or both of the backup options:
 - Select Configuration to back up important definitions.
 - Select Data to back up all data.
- Backing up both configuration and data is recommended for most deployments. In deployments where the data is not needed, for example if the data collected by Guardium is sent to another system for processing, backing up only the configuration and excluding the data is faster and produces a smaller backup file.
- Warning: If data is not backed up, it cannot be restored later.
4. Click Save to verify and save the configuration changes. The system verifies the configuration by sending a test data file to your chosen location for backup. If the operation fails, the configuration is not saved and an error message is displayed.
 5. Click Run Once Now to run the operation once.

What to do next

Go to Manage > Reports > Data Management > Aggregation/Archive Log. Verify that the operation has Succeeded.

Previous topic: [Purging system data from managed units](#)

Next topic: [Applying the upgrade patch on managed units](#)

Applying the upgrade patch on managed units

Upgrade your managed unit by distributing the upgrade patch from the central manager. Upgrade the aggregators first before you upgrade collectors.

Before you begin

Ensure that the upgrade patch is installed on your central manager.

Procedure

1. On your central manager, go to Manage > Central Management > Central Management
2. Select your managed units and click Patch Distribution.
3. Select the patch to distribute and click Install Patch Now to install the patch immediately. To schedule the installation later, click Schedule Patch.

Previous topic: [Backing up a managed unit](#)

Next topic: [Installing maintenance patches on managed units](#)

Installing maintenance patches on managed units

Distribute the maintenance patches to your managed units by using the Central Management page on the central manager.

Before you begin

Ensure that all relevant maintenance patches such as the latest bundle, security fix, and sniffer patch are installed on your central manager.

Procedure

1. On your central manager, go to Manage > Central Management > Central Management
2. Select your managed units and click Patch Distribution.
3. Select the patch to distribute and click Install Patch Now to install the patch immediately.

Previous topic: [Applying the upgrade patch on managed units](#)

Upgrading S-TAP agents in a managed environment

After you upgrade your central manager and managed units, upgrade your S-TAP agent.

Procedure

For information on upgrading UNIX S-TAPs, see:

- [Upgrading an S-TAP agent with GIM Setup by Client](#)
- [Upgrading S-TAP using RPM](#)
- [Upgrading the S-TAP agent using the shell installer](#)

For information on upgrading Windows S-TAPs, see:

- [Upgrading S-TAP agent with GIM Setup by Client](#)
- [Upgrading the S-TAP agent using the interactive installer](#)
- [Upgrading S-TAP using the command line](#)

Previous topic: [Upgrading the managed unit](#)

Upgrading a stand-alone system

Upgrade your stand-alone system to the next major version.

1. [Preparing for upgrade in a stand-alone environment](#)

The upgrade patch promotes your Guardium system to the next major version. Use the following workflow to prepare your stand-alone system for upgrade.

2. [Applying the health check patch on stand-alone systems](#)

The health check patch performs preliminary checks on your Guardium system to prevent potential issues during the upgrade. This patch must be successfully installed on your stand-alone system in the last seven days before you install the Guardium upgrade patch.

3. [Archiving data from stand-alone systems](#)

You can archive the audit data that is captured by your Guardium system to another location. These archived files can be restored later for forensic purposes without replacing the audit data that is already available in your Guardium system. Use the following procedure to archive data on your stand-alone system.

4. [Purging system data from stand-alone systems](#)

Purging unnecessary data from your stand-alone system can significantly speed up the upgrade process. For best performance and to minimize risks that are associated with upgrading large amounts of data, try to achieve less than 20% internal database utilization by purging unnecessary system data.

5. [Backing up a stand-alone system](#)

System backups store all the necessary data and configuration values to restore your Guardium system. Use this procedure to back up your stand-alone system.

6. [Applying the upgrade patch on stand-alone systems](#)

To upgrade your stand-alone Guardium system, you must install the upgrade patch. You can install the patch from your local system, from a network location, from a file server, or by using media such as a CD or DVD.

7. [Installing maintenance patches on stand-alone systems](#)

After you upgrade your Guardium system, apply the relevant maintenance patches.

8. [Upgrading S-TAP agents in a stand-alone environment](#)

After you upgrade your stand-alone system, upgrade your S-TAP agent.

Preparing for upgrade in a stand-alone environment

The upgrade patch promotes your Guardium® system to the next major version. Use the following workflow to prepare your stand-alone system for upgrade.

Procedure

1. Ensure that you meet the minimum system requirements. For more information, see [Hardware requirements](#).
2. Plan your upgrade strategy. For more information, see [Planning an upgrade](#).
3. Identify your upgrade path and download the relevant patches from the IBM Fix Central website. For more information, see [Identifying the correct upgrade path](#).
 - The latest applicable health check patch.
 - The latest upgrade patch or GPU.
 - All applicable maintenance patches, such as the latest bundle, security fix, and sniffer patch. To view the list of available patches, access the home page of the Guardium UI and click the bell icon.
 - Base and append licenses.
4. Upgrade your firmware to the most recent version provided by your vendor. If you use a Guardium appliance, check the Fix Central website for the latest firmware.
5. If you want to use an external storage system for your archive and backup, ensure that you have the configuration details ready. For more information, see [Configuring external storage](#).
6. Unmount all media such as DVDs or USB disks that are mounted either directly or virtually on the physical appliance. Mounted media might cause the upgrade to fail.
7. Schedule the installation during a quiet time on your Guardium system to avoid conflicts with other long-running processes such as heavy reports, audit processes, backups, and imports.
8. Set the time to the local time zone and synchronize time across all your Guardium systems and agents by using a Network Time Protocol (NTP) server.

Next topic: [Applying the health check patch on stand-alone systems](#)

Related information

-  [Understanding Guardium patch types and patch names](#)

Applying the health check patch on stand-alone systems

The health check patch performs preliminary checks on your Guardium® system to prevent potential issues during the upgrade. This patch must be successfully installed on your stand-alone system in the last seven days before you install the Guardium upgrade patch.

Procedure

1. Install the patch by using the CLI command **store system patch install**. For more information, see [store system patch install](#).
2. When prompted, select the health check patch from the list of available patches.
3. Monitor the installation by using the CLI command **show system patch installed**.

If the health check patch is an incorrect version, the installation fails with the error message Patch Installation Failed - Latest patch *patch_version_number* required.

Previous topic: [Preparing for upgrade in a stand-alone environment](#)

Next topic: [Archiving data from stand-alone systems](#)

Related concepts

- [System CLI commands](#)

Archiving data from stand-alone systems

You can archive the audit data that is captured by your Guardium® system to another location. These archived files can be restored later for forensic purposes without replacing the audit data that is already available in your Guardium system. Use the following procedure to archive data on your stand-alone system.

Procedure

1. Go to Manage > Data Management > Data Archive.
2. Select the Archive checkbox.
3. In the Archive data older than field, enter a value and select a unit of time from the menu.
For example, to archive data from yesterday, enter the value 1, and select Day(s) from the menu.
Tip: If you archive data on a schedule, check your archive log by accessing Manage > Reports > Data Management > Aggregation/Archive Log to ensure that there are no data gaps in your archive.
4. In the Ignore data older than field, enter the time interval to archive.
For example, to archive one day's data, enter 2. Any value that is specified here must be greater than the Archive data older than value. If you leave this field blank, you archive data for **all days** older than the value specified in Archive data older than.
5. Select the Archive Values checkbox to include values from SQL strings in the archived data. If this option is not selected, the values are replaced with question mark characters and are not available after the restore operation.
6. Select the Protocol that you want to use to store your archive and enter the configuration details.

7. Click Test connection The system verifies the configuration by sending a test data file to the configured location. If the operation fails, an error message is displayed.
8. Click Save to save the configuration changes. If the operation fails, an error message is displayed and the configuration is not saved.
9. Click Run Once Now to run the operation now.

What to do next

Go to [Manage > Reports > Data Management > Aggregation/Archive Log](#) to verify that the archive operation is successful. Each archive operation shows multiple activities. Ensure that the status of each activity is Succeeded.

Previous topic: [Applying the health check patch on stand-alone systems](#)

Next topic: [Purging system data from stand-alone systems](#)

Related concepts

- [File Handling CLI Commands](#)

Related tasks

- [Configure data archive](#)
- [Configuring external storage](#)

Purging system data from stand-alone systems

Purging unnecessary data from your stand-alone system can significantly speed up the upgrade process. For best performance and to minimize risks that are associated with upgrading large amounts of data, try to achieve less than 20% internal database utilization by purging unnecessary system data.

Procedure

1. Open [Manage > Data Management > Data Archive](#).
2. Click the Purge checkbox to define a purge operation.
Important: Changes made to the Data Archive purge configuration is also applied to the Data Export purge configuration.
3. Define a Purge data older than time period.
All data older than the specified period of days, weeks, or months are purged from the system.
4. Click the Allow purge without archiving or exporting checkbox.
5. Click Save to save the configuration changes.
6. Click Run Once Now to run the purge operation and purge old system data.

What to do next

Open [Manage > Reports > Activity Monitoring > Scheduled Jobs](#) to monitor the status of the data archive job.

Previous topic: [Archiving data from stand-alone systems](#)

Next topic: [Backing up a stand-alone system](#)

Backing up a stand-alone system

System backups store all the necessary data and configuration values to restore your Guardium® system. Use this procedure to back up your stand-alone system.

Before you begin

Determine whether you have sufficient disk space available for backup.

Tip:

For a successful backup, ensure that the DB utilization size < available disk space for backup.

You can use the following formula to calculate the disk space available for backup:

Available disk space for backup = free space available in your /var partition - 10% of the total size of your /var partition.

To find the disk size of your /var partition, navigate to [Manage > System View > System Monitor](#). On the Hard Disk Usage tile, click Tabular View to list the values for the total disk size, free disk space, and used disk space for your partitions.

Procedure

1. Go to [Manage > Data Management > System Backup](#).
2. Select the Protocol that you want to use for your backup and enter the configuration details.
3. Select one or both of the backup options:
 - Select Configuration to back up important definitions.
 - Select Data to back up all data.

Backing up both configuration and data is recommended for most deployments. In deployments where the data is not needed, for example if the data collected by Guardium is sent to another system for processing, backing up only the configuration and excluding the data is faster and produces a smaller backup file.

Warning: If data is not backed up, it cannot be restored later.

4. Click Save to verify and save the configuration changes. The system verifies the configuration by sending a test data file to your chosen location for backup. If the operation fails, the configuration is not saved and an error message is displayed.
5. Click Run Once Now to run the operation once.

What to do next

Go to [Manage > Reports > Data Management > Aggregation/Archive Log](#). Verify that the operation has Succeeded.
Previous topic: [Purging system data from stand-alone systems](#)
Next topic: [Applying the upgrade patch on stand-alone systems](#)

Related tasks

- [Configuring external storage](#)

Related information

- [store storage-system](#)

Applying the upgrade patch on stand-alone systems

To upgrade your stand-alone Guardium system, you must install the upgrade patch. You can install the patch from your local system, from a network location, from a file server, or by using media such as a CD or DVD.

About this task

The installation time depends on the amount of data that is involved, your system's specifications, and configurations. After the patch installation completes, the upgrade process begins automatically and the system restarts. Do not restart the system manually.

After restart, the system begins the following processes:

- Network configuration, database data migration, database startup.
- License upgrade and language setting.
- Database restart, certificate and key migration, password migration, and file clean-up.

Procedure

1. Install the patch by using the CLI command **store system patch install**. For more information, see [store system patch install](#).
2. When prompted, select the upgrade patch from the list of available patches.
3. Monitor the installation by using the CLI command **show system patch installed**. After installation is complete, the system restarts automatically.

Previous topic: [Backing up a stand-alone system](#)

Next topic: [Installing maintenance patches on stand-alone systems](#)

Related concepts

- [System CLI commands](#)

Installing maintenance patches on stand-alone systems

After you upgrade your Guardium® system, apply the relevant maintenance patches.

Procedure

1. Install the patch by using the CLI command **store system patch install**. For more information, see [store system patch install](#).
2. Select the maintenance patch to install.

What to do next

Repeat the procedure to install all the relevant maintenance patches.
Previous topic: [Applying the upgrade patch on stand-alone systems](#)
Next topic: [Upgrading S-TAP agents in a stand-alone environment](#)

Related information

-  [Understanding Guardium patch types and patch names](#)

Upgrading S-TAP agents in a stand-alone environment

After you upgrade your stand-alone system, upgrade your S-TAP agent.

Procedure

For information on upgrading UNIX S-TAPs, see:

- [Upgrading an S-TAP agent with GIM Setup by Client](#)
- [Upgrading S-TAP using RPM](#)
- [Upgrading the S-TAP agent using the shell installer](#)

For information on upgrading Windows S-TAPs, see:

- [Upgrading S-TAP agent with GIM Setup by Client](#)
- [Upgrading the S-TAP agent using the interactive installer](#)
- [Upgrading S-TAP using the command line](#)

Previous topic: [Installing maintenance patches on stand-alone systems](#)

Deploying Guardium on a cloud service

IBM® Guardium® offers data activity monitoring, vulnerability assessment capabilities and more on several cloud platforms.

For a list of supported cloud platforms, see [System requirements](#).

For more information about deploying a Guardium instance on a specific cloud platform, see the deployment guide for that platform in [Deploying Guardium in the cloud](#).

In addition to the Guardium instance, you might need to download updates for S-TAPs or other components from Fix Central. For more information, see [IBM Support Fix Central](#).

Important: Upgrading multi-cloud images directly from Guardium v10.x to v11.0 or later is supported only for AWS. If your site uses Guardium v10.x with another cloud platform, you cannot directly upgrade the Guardium images to v11.

If you try to upgrade, the instance becomes inaccessible and irretrievable. To upgrade images on these platforms to v11.0 or later:

1. Start a new v11 image.
 2. Back up and restore from your Guardium system as described in [System Backup](#).
-

CLI Commands

The Guardium® command line interface (CLI) is an administrative tool that allows you to configure, troubleshoot, and manage your Guardium system.

- [**Using the CLI**](#)
Learn how to access the CLI, and understand the command syntax, and the types of commands.
- [**Aggregator CLI Commands**](#)
This section lists Aggregator CLI commands.
- [**Alerter CLI Commands**](#)
This section describes the Alerter CLI commands.
- [**Certificate CLI Commands**](#)
Use the certificate commands to create a certificate signing request (CSR), and to install server certificates, CA (certificate authority) certificates, or trusted path certificates on the Guardium system.
- [**Configuration and control CLI commands**](#)
Use the following CLI commands for configuration and control.
- [**diag CLI command**](#)
Use the **diag** CLI command to access troubleshooting and maintenance utilities through the SQLGuard Diagnostics interface.
- [**File handling CLI Commands**](#)
Use these commands to backup and restore system information. Many of these tasks can be performed from Guardium user interface.
- [**Inspection Engine CLI Commands**](#)
Use these CLI commands to configure the inspection engines.
- [**Investigation Dashboard CLI Commands**](#)
Use these CLI commands to configure the Investigation Dashboard.
- [**Network Configuration CLI Commands**](#)
Use the network configuration CLI commands to set IP addresses, handle bonding and failover, handle secondary functionality, and reset networking.
- [**Support CLI Commands**](#)
Use the following CLI commands only under the direction of Technical Support.
- [**System CLI Commands**](#)
Use these CLI commands to view and configure system settings.
- [**User account, password, and authentication CLI Commands**](#)
Use these CLI commands to configure user accounts, passwords, and authentication.

Using the CLI

Learn how to access the CLI, and understand the command syntax, and the types of commands.

Documentation Conventions

All CLI command examples are written in courier text (for example, `show system clock`).

To illustrate syntax rules, some command descriptions use dependency delimiters. Such delimiters indicate which command arguments are mandatory, and in what context. Each syntax description shows the dependencies between the command arguments by using special characters:

- Angle brackets (< >) denote a required argument.
- Square brackets ([]) denote an optional argument.
- A vertical bar (|) separates alternatives when only one can be selected. For example:

```
store full-bypass <ON | OFF>
```

CLI Command Usage

- Commands and keywords can be abbreviated by entering enough characters so the commands are not ambiguous. For example, show can be abbreviated sho.
- Most Guardium® CLI commands consist of a command word followed by one or more arguments. The argument can be a keyword or a keyword followed by a variable value (for example an IP address, subnet mask, or date).
- Commands and keywords are not case-sensitive, but element names are.
- To display command syntax and usage options, enter a question mark (?) as an argument that follows the command word.
- Use quotation marks around words or phrases to precisely define search terms.

Accessing the CLI

An administrator can access the CLI through either:

- A network connection that uses an SSH client.
- A physically connected PC console or serial terminal.

Network SSH Access

Remote access to the CLI is available on the management IP address or domain name, by using an SSH client. SSH clients are freely or commercially available for most desktop and server platforms. A UNIX SSH connect command to log in as the cli user might look like this:

```
ssh -l cli 192.168.2.16
```

The SSH client might display a request to accept the cryptographic fingerprint of the Guardium appliance. Accept the fingerprint to proceed to the password prompt.

Note: If you are asked again for a fingerprint after the first connection, someone might be trying to induce you to log in to the wrong machine.

Physical Console Access

Interactive access to the Guardium appliance is through the serial port or the system console.

- PC keyboard and monitor: A PC video monitor can be attached to either the front panel video connector or the video connector on the back of the appliance.
- A PC keyboard with a USB keyboard can be connected to the USB connectors at the front or back of the appliance.
- Serial port access: Use a NULL modem cable to connect a terminal or another computer to the 9-pin serial port at the back of the appliance. Set the terminal or a terminal emulator on the attached computer to communicate as 19200-N-1 (19200 baud, no parity, 1 stop bit).

A login prompt displays after the terminal is connected to the serial port, or the keyboard and monitor are connected to the console. Enter `cli` as the user name, and continue with CLI Login.

CLI Login

Access the CLI through the admin CLI account `cli` or one of the special `guardcli` accounts (`guardcli1`, ..., `guardcli9`). The `guardcli` accounts are available to help you separate administrative duties.

Access to the GuardAPI requires that the access manager create a user (GUI username/`guiuser`) with either the admin or CLI role. To log into the CLI to use GuardAPI commands, the user must first log in with one of the CLI accounts (`guardcli1`, ..., `guardcli9`) and then log in with their own user name to the `guiuser` by issuing the `set guiuser` command. For more information, see [Using GuardAPI commands](#) or [Authenticating GuardAPI commands with set guiuser command](#).

In addition, if multi-factor authentication is set up for your site, an additional message displays after you log in.

Password Hardening

To meet various auditing and compliance requirements, the following password rules are in place for CLI accounts:

- For the account `cli` either use the CLI password that is supplied or be sure to set a strong password to protect this account. If you rebuild the system, the Guardium `cli` user has a default password of `guardium`. Change the password immediately.
- Passwords expire for the CLI and `guardcli` accounts every 90 days by default. Passwords for your site might be different, depending on the values of the [store password_expiration](#) CLI command. After a password expires, you must change the password when you next log in.
- Passwords must be a minimum of 8 characters long. Depending on the value of the [enable_strong_cli_password](#) API command, the password minimum for the `cli` user might be 15 characters.
- Passwords must contain at least one character from three of the following four categories:
 - Any uppercase letter
 - Any lowercase letter
 - Any number (0,1,2,...)
 - A non-alphanumeric (special) character as described in [Special characters for Guardium passwords](#)

- After access is granted by using a separate GUI username (guiuser), the CLI audit trail shows the CLI_USER+GUI_USER pair that was used to log in.

Limited CLI commands during maintenance of internal database

CLI has three sets of commands - general commands, specialized support commands, and recovery commands. Technical support uses the support commands to analyze the system. Recovery commands help recover the system when the database is down.

The initial CLI login is:

```
Welcome to CLI - your last login was <date>
```

The welcome message will add further information if the internal database is down due to maintenance or during an upgrade.

In this case, the number of CLI commands available are limited.

```
The internal database on the appliance is currently down and CLI will be working  
in "recovery mode"; only a limited set of commands will be available.
```

The following CLI commands are available for use during recovery mode:

```
support reset-password root  
restart mysql  
restart stopped_services  
restart system  
restore backup  
restore pre-patch-backup
```

Aggregator CLI Commands

This section lists Aggregator CLI commands.

aggregator backup keys file

Use this command to back up the shared secret keys file to the specified location.

Syntax

```
aggregator backup keys file <user@host:/path/filename>
```

Parameters

`user@host:/path/filename` For the file transfer operation, specifies a user, host, and full path name for the backup keys file. The user you specify must have the authority to write to the specified directory.

Note: For more information about the shared secret use, see System Shared Secret.

aggregator clean shared-secret

Sets the system shared secret value to null. All files archived or exported from a unit with a null shared secret can be restored or imported only on systems where the shared secret is null.

Syntax

```
aggregator clean shared-secret
```

Note: For more information about the shared secret use, see System Shared Secret.

aggregator debug

Starts or stops writing debugging information relating to aggregation activities. Use these commands only when directed to do so by Guardium® Support, and be sure to issue the stop command after you have gathered enough information.

Note: Debug mode will automatically expire after 7 days.

Syntax

```
aggregator debug <start | stop>
```

aggregator list failed imports

When an import operation fails because of a shared secret mismatch, the offending file is moved from the /var/importdir directory to the /var/dump directory, and it is renamed using the original file name plus the suffix .decrypt_failed. Use this command to list all such files.

Syntax

```
aggregator list failed imports
```

aggregator recover failed import

Use this command to move and rename failed import files, prior to re-attempting an import or restore operation. Failed import files are stored in the /var/dump directory, with the suffix .decrypt_failed. Before re-attempting an import or restore operation, those files must be renamed (by removing the .decrypt_failed suffix) and moved to the

/var/importdir directory.

Syntax

```
aggregator recover failed import <all | filename>
```

Parameters

Use the all option to move all files from the /var/dump directory ending with the suffix .decrypt_failed, or use the filename option to identify a single file to be moved.

Note: After moving the failed files, but before a restore or import operation runs, be sure that the system shared secret matches the shared secret used to encrypt the exported or archived file.

[**aggregator restore keys file**](#)

Use this command to restore the shared secret keys file from the specified location.

Syntax

```
aggregator restore keys file <user@host:/path/filename>
```

Parameters

user@host:/path/filename For the file transfer operation, specifies a user, host, and full path name for the backup keys file.

Note: For more information about the shared secret use, see System Shared Secret.

[**store aggregator drop_ad_hoc_audit_db**](#)

Audit Process reports on Aggregator – creates ad-hoc databases for each of its tasks that will include only the relevant days for that task. These ad-hoc databases can be kept for 14 days (for analysis) or deleted immediately after use. The CLI command defines the ad-hoc databases purging policy. Choices are 0 or 1(0 - keep for 14-days or 1 - delete after use).

Syntax

```
store aggregator drop_ad_hoc_audit_db [1|0]
```

Drop ad-hoc merge databases? 0

```
show aggregator drop_ad_hoc_audit_db
```

[**store aggregator orphan_cleanup_flag**](#)

Use this CLI command to regularly run static orphans cleanup on an aggregator.

Use this CLI command to clean orphans on aggregators that will be scheduled to run on data older than 3 days and will run at the end of a purge.

This process will be started by the user with this CLI command, so in case of large database, the user will be aware of the time length of the process.

It will cover the whole data on the aggregator, but will run it all on a separate temporary database.

Note: On a collector, orphans cleanup is not changed - it runs with the small cleanup tactics and is invoked before export/archive.
show aggregator orphan_cleanup_flag Displays small, large or analyze.

```
store aggregator orphan_cleanup_flag
```

```
store aggregator orphan_cleanup_flag <flag>, where flag is one of the words < small large analyze >
```

These commands are applicable on aggregator only.

If set to one of small, large or analyze - orphans cleanup script is invoked after each run of merge process.

The orphans cleanup on an aggregator does not remove orphan records of the last 3 days - it does remove all orphans older than 3 days.

If small is specified, the process does not interfere with audit processes that can start after the merge is completed.

If large is specified, the process would run faster where there is a large number of orphans but it's run might interfere with audit processes - if large is specified, audit processes will not start until orphans cleanup is complete.

If analyze is specified, the process first evaluates the number of orphans and uses the large tactics if there are more than 20% orphans - if analyze is specified, audit processes will not start until orphans cleanup is complete.

Syntax

```
store aggregator orphan_cleanup_flag [ small | large | analyze]
```

Show command

```
show aggregator orphan_cleanup_flag
```

[**store archive_static_table**](#)

Use this CLI command to turn off/ turn on the archive static table

USAGE: store archive_static_table <state>,

where state is on/off.

Show command

```
show archive_static_table
```

store next_export_static

The aggregation software makes a distinction between two types of tables:

- static tables - grow slowly over time, data in these tables is not time dependent (GDM_OBJECT, GDM_FIELD, GDM_SENTENCE, GDM_CONSTRUCT, etc.).
- dynamic tables- grow quickly with time, data is time dependent (GDM_CONSTRUCT_INSTANCE, GDM_SESSION, GDM_CONSTRUCT_TEXT etc.).

As stated previously, the data of static tables is not time dependant. The data of dynamic tables that is time dependant is linked to static data. As static tables can grow to be very large, the export/archive process does not archive the full static data every day - it archives the full static data the first time it runs, and then at the first day of each month, on any day besides the first of the month, it only archives static data that changed during that day. For this reason when restoring data of any day, it is also required that the first of the month be restored - this ensures that full static data is present and references are not broken.

Use the CLI command, store next_export_static, to set a flag so that the next export contains the full static data.

Syntax

```
store next_export_static [ON | OFF]
```

Show command

```
show next_export_static
```

store last_used

Use this CLI command during purging and aggregation.

Syntax

```
store last_used [size | interval | logging]
```

Show command

```
show last_used [size | interval | logging]
```

LAST_USED SIZE - Integer, Default is 50

LAST_USED INTERVAL - Integer, default is 60 (minutes)

LAST_USED LOGGING - Integer

All Tables - 1

Only GDM_Object - 2

None - 0 (Default)

store aggregator static_data

```
store aggregator static_data [TIMESTAMP | LAST_USED_FOR_OBJECT_ONLY | LAST_USED ]
```

Note: Set the CLI command, last_used logging, prior to using this command.

When the LAST_USED column is updated by the Sniffer in Static tables, this column can be referenced when purging data from these tables or when archiving and exporting data from these tables.

The value of this column can also be updated when importing data to an aggregator.

There are three options:

1. By default, the system behaves like it did in previous versions - the LAST_USED column is not considered in purge, archive and export and is not updated on import, archive and export are done by TIMESTAMP.
2. LAST_USED_FOR_OBJECT_ONLY is considered only for GDM_OBJECT table.
3. LAST_USED is considered for GDM_CONSTRUCT, GDM_SENTENCE, GDM_OBJECT, GDM_FIELD, GDM_JOIN, GDM_JOIN_OBJECT

Note: Options 2 and 3 are only enabled when the sniffer is configured to collect and update this data.

Note: Validations performed only on a collector - If ADMINCONSOLE_PARAMETER.LAST_USED_LOGGING=0, then only TIMESTAMP is allowed. If ADMINCONSOLE_PARAMETER.LAST_USED_LOGGING=1 then all parameters are allowed. If ADMINCONSOLE_PARAMETER.LAST_USED_LOGGING=2, then TIMESTAMP and LAST_USED_FOR_OBJECT_ONLY are allowed. On an aggregator, all parameters are allowed.

Syntax

```
store aggregator static_data <type>
```

where <type> is <TIMESTAMP | LAST_USED | LAST_USED_FOR_OBJECT_ONLY> depends on the last_used logging flag.

Use show/store last_used logging commands.

Show command

```
show aggregator static_data
```

store archive_table_by_date

Use the CLI command, store archive_table_by_date, only on Aggregators. Use this CLI command to archive all static tables on a daily basis or archive static tables data at the first time of running and every first day of the month. In default, archive data on an aggregator will run with full static tables on a daily basis. If this CLI command is set to ENABLE, static tables will be archived only on the first day of month or the first time archive data is running.

store run_cleanup_orphans_daily

Use this CLI command to clean all the old construct records that are no longer in use. This CLI command is relevant for collectors and aggregators and by default is enabled.

store run_cleanup_orphans_daily

USAGE: store run_cleanup_orphans_daily [on|off]

Show command

show run_cleanup_orphans_daily

store max_number_collector

Set the maximum number of collectors managed by aggregator. Default is 10.

Show command

show max_number_collector

store purge_age_period

Set the period of purge age.

Show command

show purge_age_period

Alerter CLI Commands

This section describes the Alerter CLI commands.

The Alerter subsystem transmits messages that are queued by other components, for example, correlation alerts that are queued by the Anomaly Detection subsystem, or run-time alerts that are generated by security policies. You can configure the Alerter subsystem to send messages to both SMTP and SNMP servers. You can also send alerts syslog or custom alerting classes, but no special configuration is required for those two options, beyond starting the Alerter. Alerter commands fall into the following categories:

- Alerter Start-up and Polling Commands
- SMTP Configuration Commands
- SNMP Configuration Commands

Note: In addition to these Alerter commands, there are configuration Alerter commands. For more information, see [Configuration and control CLI commands](#).

restart alerter

Restarts the Alerter. You can perform the same function using the store alerter state operational command to stop and then start the alerter:

store alerter state operational off

store alerter state operational on

12.0 Syntax

restart alerter

12.1 and later Syntax

restart alerter [--yes]

Where --yes causes the command to run automatically.

stop alerter

Stops the Alerter.

You can perform the same function using the store alerter state operational command:

store alerter state operational off

Syntax

stop alerter

store alerter delay

Sets the number of seconds to delay real-time alerts. The default is 300 (5 minutes), the maximum is 3600. Some real-time alert values, such as Records Affected, require that snif receive and process all response data for the alerting request. This value sets the time that the Alerter waits before processing alerts that rely on this response data.

Restart the Alerter for configuration changes to take effect.

Syntax

```
store alerter delay <n>
```

Show Command

```
show alerter delay
```

store alerter email append_name_subject

Appends the appliance name in email subject.

Syntax

```
store alerter email append_name_subject <on | off>
```

Show command

```
show alerter email append_name_subject
```

store alerter email append_subject_body

Appends the email subject in the beginning of the email body.

Syntax

```
store alerter email append_subject_body <on | off>
```

Show command

```
show alerter email append_subject_body
```

store alerter poll

Sets the number of seconds, n, that the Alerter waits before checking its outgoing message queue to send SNMP traps or transmit email using SMTP. The default is 30. Restart the Alerter for configuration changes to take effect.

Syntax

```
store alerter poll <n>
```

Show Command

```
show alerter poll
```

store alerter smtp authentication password

Sets the alerter SMTP authentication password to the specified value. There is no corresponding show command. Restart the Alerter for configuration changes to take effect.

Syntax

```
store alerter smtp authentication <value>
```

store alerter state operational

Starts or stops the Alerter. The default state at installation time is off. You can also use the **restart alerter** or **stop alerter** commands to restart or stop the Alerter subsystem.

Syntax

```
store alerter state operational <on | off>
```

Show Command

```
show alerter state operational
```

store alerter state startup

Enables or disables the automatic start-up of the Alerter on system start-up. The default state at installation time is off.

Syntax

```
store alerter state startup <on | off>
```

Show Command

```
show alerter state startup
```

store anomaly-detection poll

Sets the Anomaly Detection polling interval, in minutes (n). This controls the frequency with which Guardium® checks log data for anomalies.

Syntax

```
store anomaly-detection poll <n>
```

Show Command

```
show anomaly-detection poll
```

store alerter smtp authentication type

Sets the authentication type required by the SMTP server to the one of the following values:

- none: Send without authentication.
- auth: Username/password authentication. Set the user account and password using the following commands:
 - store alerter smtp authentication username
 - store alerter smtp authentication password

Restart the Alerter for configuration changes to take effect.

Syntax

```
store alerter smtp authentication type <none | auth>
```

Show Command

```
show alerter smtp authentication type
```

store alerter smtp authentication username

Sets the alerter SMTP email authentication username to the specified name.

Syntax

```
store alerter smtp authentication username <name>
```

Show Command

```
show alerter smtp authentication username
```

store alerter smtp port

Sets the port number on which the SMTP server listens, to the value specified by n. The default is 25 (the standard SMTP port). Restart the Alerter for configuration changes to take effect.

Syntax

```
store alerter smtp port <n>
```

Show Command

```
show alerter smtp port
```

store alerter smtp relay

Sets the IP address of the SMTP server to be used by the Guardium appliance. Restart the Alerter for configuration changes to take effect.

Syntax

```
store alerter smtp relay <ip address>
```

Show Command

```
show alerter smtp relay
```

store alerter smtp returnaddr

Sets the return email address for email alerts. Any bounced messages or email failures will be returned to this address.

Syntax

```
store alerter smtp returnaddr <email address>
```

Show Command

```
show alerter smtp returnaddr
```

store alerter smtp starttls

Sets encryption for the email server.
Note: For SMTP, TLS works over port 587.
Syntax

```
store alerter smtp starttls < TLS | SSL | none >
• none: No encryption is required.
• SSL: Sets TLS data encryption.
• TLS: Sets TLS data encryption.
```

Show command

```
show alerter smtp starttls
```

store alerter snmp community

Sets the SNMP trap community used by the Alerter, to the name specified. There is no corresponding show command.

Syntax

```
store alerter snmp community <name>
```

store alerter snmp secondary_community

Sets a secondary SNMP trap community used by the Alerter, to the name specified. There is no corresponding show command.

Syntax

```
store alerter snmp secondary_community <string>
```

Where string is the text community string.

store alerter snmp traphost

Sets the Alerter SNMP trap server to receive alerts, to the specified IP address or DNS host name.

Syntax

```
store alerter snmp traphost <snmp host>
```

Show Command

```
show alerter snmp traphost
```

store alerter snmp secondary_traphost

Sets a secondary Alerter SNMP trap server to receive alerts to the specified IP address.

Syntax

```
store alerter snmp secondary_traphost <arg>
```

Where <arg> is the IP address of the secondary SNMP server or the word "null" to reset value.

Show Command

```
show alerter snmp secondary_traphost
```

store anomaly-detection state

Enables or disables the Anomaly Detection subsystem, which executes all active statistical alerts, checks the logs for anomalies, and queues alerts as necessary for the Alerter subsystem.

Syntax

```
store anomaly-detection state <on | off>
```

Show Command

```
show anomaly-detection state
```

Certificate CLI Commands

Use the certificate commands to create a certificate signing request (CSR), and to install server certificates, CA (certificate authority) certificates, or trusted path certificates on the Guardium® system.

Note: Guardium does not provide certificate authority (CA) services and does not deliver systems with different certificates than the one installed by default. If you want your site to have its own certificate, you must contact a third-party CA (such as VeriSign or Entrust).

Certification Expiration

Expired certificates result in a loss of function. Run the **show certificate warn_expire** command periodically to check for expired certificates. The command displays certificates that expire within six months and already-expired certificates. The user interface also informs you of certificates that are due to expire. To see a summary of all certificates, run the command **show certificate summary**.

New Certificates

To obtain a new certificate, generate a certificate signed request (CSR) and contact a third-party certificate authority (CA) such as VeriSign or Entrust. Guardium does not provide CA services and does not ship systems with different certificates than the ones that are installed by default. The certificate format must be in PEM and include BEGIN and END delimiters. You can either paste the certificate from the console or import it through one of the standard import protocols.

Note: Do not create the CSR until after the system network configuration parameters are set.

create csr

Creates a certificate signing request (CSR) for the Guardium system. Do not create the CSR until after the system network configuration parameters are set. Within the generated CSR, the common name (CN) is created automatically from the host and domain names assigned.

Note: Where indicated, specify the rfc7468 parameter to generate a CSR that conforms to RFC 7468 formatting. Some CAs, such as the Amazon Web Services (AWS) CA, require RFC 7468 format. Check with your CA to determine whether RFC7468 formatting is accepted or required.

Note: The following CLI commands support the subject alternative name (SAN): **create csr alias**, **create csr external_stap**, **create csr gim**, and **create csr gui**. There are 100 SAN slots for each CSR generation command. 99 of the SANs are optional and can be added in FQDN (Fully Qualified Domain Name) format. The first SAN slot is reserved for the common name.

Parameters

`create csr alias [rfc7468]`

Creates a certificate signing request CSR for a supplied alias.

`create csr external_stap [rfc7468]`

Creates a CSR for a Guardium External S-TAP® Docker container. After a certificate is signed and stored, you can deploy the External S-TAP to monitor traffic from databases in the cloud or in other situations in which you cannot use a local agent.

Note: As of Guardium V11.0, the `create csr gim` client and `create csr gim server` CLI commands replace `create csr gim`.
`create csr gim client [rfc7468]`

Creates a CSR with the alias gim in the GIM client keystore. Used for centralized GIM certificate distribution. See [Manage GIM certificate distribution](#).

`create csr gim server [rfc7468]`

Creates a CSR with alias gim for the GIM server certificate. Used for centralized GIM certificate distribution. See [Manage GIM certificate distribution](#).

`create csr gui`

Creates a CSR for the GUI.

`create csr gui [custom-dn | rfc7468]`

Where:

- `custom-dn` - Creates a CSR for the GUI with a custom distinguished name (DN). The DN is a name that uniquely identifies an entry and includes a slash-separated (/) string of identifiers. For example:

`/C=US/OU=Guardium Appliances/OU=Example/CN=mycompany.com`

The DN must be ASCII-encoded and end with a CN (common name) entry.

- `rfc7468` - Creates a CSR for the GUI with RFC7468 formatting.

`create csr insights`

Creates a CSR for IBM® Guardium Insights.

`create csr mysql`

Creates a CSR for a MySQL certificate.

`create csr saml`

Creates a CSR for SAML certificates.

`create csr sniffer`

Creates a CSR for sniffer.

`create csr sniffer custom-dn`

Creates a CSR for sniffer with a custom distinguished name (DN). The DN is a name that uniquely identifies an entry and includes a slash-separated (/) string of identifiers. For example,

`/C=US/OU=Guardium Appliances/OU=Example/CN=mycompany.com`

The DN must be ASCII-encoded and end with a CN (common name) entry.

`create csr wildcard [rfc7468]`

Generates a wildcard CSR certificate. For example, if your site has machines that are named nyc.yourdomain.com, la.yourdomain.com, and tokyo.yourdomain.com, use a wildcard certificate to specify the hostname with an asterisk (*) wildcard. The wildcard creates a certificate that is valid for all three machines. For example, *.yourdomain.com.

To generate a CSR (Certificate Signing Request) wildcard certificate:

1. On the central manager (in a managed environment), run the **create csr wildcard** command.
 2. Copy the CSR into a file and get it signed by a CA.
 3. Store the signed certificate by using the **store certificate gui** CLI command. The certificate must be in PEM format in order to import it into the Guardium appliance. Make sure that you have the root CA available.
 4. In a centrally managed environment, add the certificate to each managed unit,
 - a. Store the root CA by running the **store certificate keystore** CLI command on the managed unit that uses the same root CA as you used for the central manager.
 - b. Store both the certificate and the private key with the **store certificate privatekey gui** command with the same wildcard certificate that you used for the central manager.
- Note: Use the **show csr wildcard** CLI command to view the privatekey.

Note: The Common Name for wildcard certificates must always start with an asterisk.

Syntax

- **create csr alias [rfc7468]**
- **create csr external_stap [rfc7468]**
- **create csr gim [client | server] [rfc7468]**
- **create csr gui [custom-dn | rfc7468]**
- **create csr insights**
- **create csr mysql**
- **create csr saml**
- **create csr sniffer [custom-dn]**
- **create csr wildcard [rfc7468]**

Show command

show csr wildcard key

create self-signed gui

Use this command to manually create a self-signed certificate that uses the fully qualified domain name (FQDN) of the Guardium system. Before you use this command, set the hostname and domain name.

Syntax

create self-signed gui <force>

The parameter force creates a new self-signed certificate even if a certificate exists on the Guardium system. Nondefault certificates are removed.

delete certificate

Use this command to remove SSL certificates that are expired or revoked.

Note: Use caution when you delete certificates. If a GUI certificate is deleted in error, you cannot connect to the GUI until the certificate is restored. For more information about restoring certificates, see [restore certificate keystore](#).

Parameters

Syntax

delete certificate <external_stap | external_stap_signing | keystore>

Where:

- **external_stap** displays all of the available certificates for the External S-TAP.
- **external_stap_signing** displays aliases of all available intermediate certificates for External S-TAP and prompts you to select the certificate to delete.
- **keystore** displays all certificates in the certificate keystore.

When prompted, select the number of the certificate to delete. To delete more than one certificate, enter a comma-separated list of the certificate numbers.

distribute certificate showlog

Use this command to view the certificate distribution log.

Syntax

distribute certificate showlog <all | fail | success>

where:

- **all** displays all the lines in the distribution log.
- **fail** displays the lines with failures and warnings only.
- **success** displays the lines with success only.

replace certificate

12.1 and later Replaces the GIM certificates that is installed by default with SHA1 or SHA256. The GIM client and the server do not lose communication.

```
replace certificate gim algorithm
```

USAGE:**replace certificate gim algorithm < default | default_sha1 >**, where 'default' represents SHA256 and 'default_sha1' represents SHA1 signature algorithm.

restore certificate

Parameters

```
restore certificate insights <default | last>
```

Restores the Guardium Insights certificate to either the default certificate keystore or to the last saved certificate keystore.

```
restore certificate keystore <backup | default>
```

Restores the certificate keystore to the last certificate keystore on record or the default certificate keystore that was originally provided.

- restore certificate keystore backup

Restores the certificate keystore to the last saved certificate keystore.

- restore certificate keystore default

Restores the certificate keystore to the default value that was supplied with the system.

```
restore certificate mysql backup <client <ca|cert> | server <ca|cert>>
```

Restores the last saved MySQL certificate. Specify which certificate you want to restore; the client or server certificate and the certificate authority (CA) or client certificate.

- restore certificate mysql backup client ca

Restores the last saved client certificate authority (CA) certificate.

- restore certificate mysql backup client cert

Restores the last saved client certificate.

- restore certificate mysql backup server ca

Restores the last saved server certificate authority (CA) certificate.

- restore certificate mysql backup server cert

Restores the last saved server certificate.

```
restore certificate sniffer <backup | default>
```

Restores the certificate to either the last saved sniffer certificate (the backup) or the default certificate.

Syntax

- restore certificate insights < default | last >

- restore certificate keystore <backup | default>

- restore certificate mysql backup <client | server> <ca | cert>

- restore certificate sniffer <backup | default>

restore cert_key

```
restore cert_key mysql backup <client | server>
```

Restores the MySQL client or server certificate key to the last saved value.

```
restore cert_key sniffer <backup | default>
```

12.0 This command is deprecated in Guardium 12.1.

Restores the sniffer certificate key to the last saved certificate key (backup) or the default sniffer certificate key.

Syntax

```
restore cert_key mysql backup <client | server>
```

```
restore cert_key sniffer <backup | default>
```

show certificate

Displays the summary of all certificates, certificate information, alias list, certificates in the keystore, and expired or soon-to-expire certificates.

This certificate authenticity can be verified by a Guardium CA public key (contained in the CA certificate that is distributed with the client software). The certificate has either a customer company-unique CN (Common Name - for example, acme.com), or a machine-specific CN (for example x4.acme.com). This permits any client to establish that the Guardium system has a valid certification (it is a real Guardium system), but also that it is a specific Guardium system (or a set of Guardium systems) that the client is supposed to connect to.

Parameters

```
show certificate all
```

Displays all the certificates on the Guardium appliance.

```
show certificate external_stap
```

Displays a summary of External S-TAP certificates, including certificate information, alias, certificates in the keystore, and expired or soon-to-expire certificates.

```
show certificate external_stap_signing
```

Displays a summary of External S-TAP intermediate certificates, including certificate information, alias names, certificates in the keystore, and expiration information.

```
show certificate gim client
Displays the GIM client certificate or certificates.

show certificate gim server
Displays the GIM server certificate.

show certificate gui
Displays the GUI certificate.

show certificate insights
Displays all Guardium Insights certificates that are stored in the Guardium Insights keystore

show certificate keystore alias
Displays a list of certificates. Select a certificate from the list to display its alias.

show certificate keystore all
Displays all the certificates in the Guardium keystore.

show certificate mysql client
Displays the MySQL client certificate.

show certificate mysql server
Displays the MySQL server certificate.

show certificate saml
Displays the SAML certificate.

show certificate sniffer
Displays the sniffer certificate.

show certificate starttls
Displays an existing starttls certificate.

show certificate squid
show certificate summary
Displays a summary of all certificates on the Guardium appliance.

show certificate trusted
Displays all trusted certificate information.

show certificate warn_expired
Displays all expired certificates or certificates that expire in 6 months.

show certificate wkc
Displays the certificate that is required for IBM Knowledge Catalog integration.
```

Syntax

- show certificate all
- show certificate external_stap
- show certificate external_stap_signing
- show certificate gim <client | server>
- show certificate gui
- show certificate insights
- show certificate keystore <alias | all>
- show certificate mysql <client | server>
- store certificate saml
- show certificate sniffer
- show certificate starttls
- show certificate summary
- show certificate trusted
- show certificate warn_expired
- show certificate wkc

store certificate

Stores a certificate. Follow the directions to paste your certificate (in PEM format) and include the BEGIN and END lines.

All certificates except for GIM client and GIM server are merged into the main keystore during the store certificate operation.

Note: Where [console | external] is specified, use console to paste the content to the console; use external to import a certificate located externally. The default is console.

Parameters

```
store certificate allowlist_external_stap
For the External S-TAP, stores trusted certificates. For more information, see Client and server certificate verification.
store certificate blocklist_external_stap
For the External S-TAP, store certificates that you know cannot be trusted. For more information, see Client and server certificate verification.
store certificate cms
For managing GUI and GIM certificates by using the Venafi certificate management system. For more information, see Managing certificates by using Venafi.
store certificate custom_keystore_external_stap
Store certificates in the custom keystore to verify that the External S-TAP communicates only with trusted clients and servers. For more information, see Client and server certificate verification.
store certificate external_stap
Stores the signed External S-TAP certificate into the corresponding keystore. For more information, see External S-TAP.
store certificate external_stap_signing
Stores the signed intermediate External S-TAP certificate into the corresponding keystore. For more information, see External S-TAP.
store certificate gim client [auto-generate|console|external]
Stores the signed GIM client certificate into the corresponding keystore and prepares it for distribution. Used for centralized GIM certificate distribution. See Manage GIM certificate distribution. Unlike all other certificates, storing the GIM client certificate does not affect the main keystore. Instead, the GIM client keystore is saved in a custom keystore that can be distributed to registered GIM clients.
Use auto-generate to generate and distribute selected GIM client certificates. You can generate only SHA-1 certificates. You do not need to use this command to generate SHA-256 certificates.
store certificate gim server [console|external]
Stores the signed GIM server certificate into the keystore. Used for centralized GIM certificate distribution. See Manage GIM certificate distribution.
store certificate gui
Stores a GUI certificate in the keystore.
store certificate insights [console | external | trusted]
Stores a Guardium Insights certificate in the keystore, where:


- console - Paste the certificate to the console.
- external - Import an externally generated certificate.
- trusted - Paste a trusted CA certificate to the console.


store certificate keystore_external_stap
Stores root and intermediate trusted certificates, which are used to sign External S-TAP certificates.
store certificate keystore [alias | trusted | trusted-venafi] [console|external]
Store certificates on the keystore. You can store the certificate alias, a trusted certificate, or a trusted Venafi certificate. Specify trusted to store CA certificates for TLS validation.
store certificate mysql
Stores MySQL client and server certificates. For both client and server certificates, specify ca to store certificate authority (CA) certificates. Specify cert to store client or server default certificates.


- store certificate mysql client <ca|cert> [console|external]
      Stores MySQL client certificates.
- store certificate mysql server <ca|cert> [console|external]
      Stores MySQL server certificates.



Storing certificates with private key



The following commands overwrite self-signed GUI, GIM, and Insights certificates with private keys in the keystore.



Note:  
Certificates and private keys must be in PEM format.



Certificates start with "-----BEGIN CERTIFICATE-----" and end with "-----END CERTIFICATE-----"



Private keys start with "-----BEGIN RSA PRIVATE KEY-----" and end with "-----END RSA PRIVATE KEY-----"



PEM certificates can also be imported by using the GUI. For more information, see Importing a PEM certificate.



store certificate privatekey gim [console | external]



Stores GIM self-signed certificate and private key in the keystore.



store certificate privatekey gui [console | external]



Stores GUI self-signed certificate and private key in the keystore.


```

Stores a Guardium Insights self-signed certificate and private key in the keystore.

Note: You must restart the Guardium Insights agent.

store certificate rsa_securid console

Stores a certificate for RSA SecurID multi-factor authentication. The certificate verifies the RSA SecurID Authentication Manager. Run this command on a central manager. SSH authentication is required for SSH logins with RSA SecurID. The certificate must be in PEM format.

After you store the certificate, use the **configure_mfa** API command to configure multi-factor authentication from the CLI.

Note: From **configure_mfa**, make sure that you set the `sslVerify` parameter to `true`. If `sslVerify` is not set to `true`, the GUI and `SET_GUIUSER` logins does not use the certificate, and for SSH logins, the **configure_mfa** API command fails.

For more information, see [Configuring multi-factor authentication with RSA SecurID](#).

store certificate saml

Stores SAML certificates.

store certificate scanner ca_bundle <agent>

Stores the certificate for the CVE scanner agent. For more information, see [Configuring vulnerability scanner agents](#).

store certificate sniffer

Stores sniffer certificates.

store certificate starttls [console | external]

Store a trusted certificate in the keystore to support an encrypted TLS connection.

store certificate wkc [console | external]

Required for the Guardium and IBM Knowledge Catalog integration. Use this command to store the IBM Cloud Pak® for Data root CA certificate, which is required to connect to your IBM Knowledge Catalog environment.

Important: The Cloud Pak for Data installation includes a self-signed certificate. Do not use the self-signed certificate in a production environment. Acquire and install a CA-signed certificate for production use.

For more information about obtaining and using a Cloud Pak for Data certificate, see [Using a custom TLS certificate for HTTPS connections to the platform](#) in the IBM Cloud Pak for Data documentation.

For more information about using the IBM Knowledge Catalog integration, see [Integrating with IBM Knowledge Catalog for federated data protection](#) and [store_wkc_configuration](#).

Note: This command is available only on managed units and stand-alone machines.

Syntax

- store certificate allowlist_external_stap
- store certificate blocklist_external_stap
- store certificate cms
- store certificate custom_keystore_external_stap
- store certificate external_stap
- store certificate external_stap_signing
- store certificate gim client [auto-generate|console|external]
- store certificate gim server [console|external]
- store certificate insights [console|external|trusted]
- store certificate keystore <alias | trusted> [console|external]
- store certificate keystore_external_stap
- store certificate mysql client <ca|cert> [console|external]
- store certificate mysql server <ca|cert> [console|external]
- store certificate privatekey <gim | gui > [console|external]
- store certificate rsa_securid console
- store certificate saml
- store certificate scanner ca_bundle
- store certificate sniffer
- store certificate starttls [console | external]
- store certificate wkc [console | external]

store cert_key mysql

Stores the certificate key of a MySQL client or server. Specify `console` to paste the key into the console. Specify to import the key file from an external source. Specify to import the key file from an external source.

Parameters

Use the following parameters to store the certificate key of a MySQL client:

store cert_key mysql client [console|external]

Use the following parameters to store the certificate key of a MySQL server:

store cert_key mysql server [console|external]

store cert_key sniffer

12.0 This command is deprecated in Guardium 12.1.

If the certificate signing request (CSR) is not generated in the Guardium appliance, the **store cert_key sniffer** command prompts you to enter the key to store the certificate.

Stores the system certificate key. This command enables a user to set the system certificate that is used by the Guardium system (in communication with S-TAP). The certificate can either be pasted from the console or imported through one of the standard import protocols. Use the PEM certificate format and include the BEGIN and END delimiters. This certificate needs to be signed by a CA whose self-signed certificate is available to S-TAP software through the `guardium_ca_path`.

Parameters

`store cert_key sniffer console`

Stores the sniffer certificate key by pasting the key into the console.

`store cert_key sniffer external`

Stores the sniffer certificate key by importing the key file from an external source.

Syntax

`store cert_key sniffer <console | external>`

Backup and Default Options

You can choose to restore certificates and certificate keys with the backup or default parameter. Use the backup parameter to restore a certificate to the last saved certificate. Use the default parameter to restore a certificate to the original certificate that Guardium supplied.

Certificate Expiration Dates and Summary Commands

Run the `show certificate warn_expire` command periodically. This command warns you of certificates that expire in six months and displays a list of expired certificates. For more information, see the **show certificate CLI** command. To show a summary of all certificates, run the CLI command `show certificate summary`. Run the commands periodically to review certificate expiration dates.

Configuration and control CLI commands

Use the following CLI commands for configuration and control.

? (question mark)

To find more information about a command, enter a question mark at any point to display the arguments.

Syntax

`<partial_command> ?`

Example

`CLI> show account strike ?`

`USAGE: show account strike <arg>, where arg is:
?, count, interval, max
ok
CLI>`

commands

Displays an alphabetical listing of all CLI commands.

Syntax

`commands`

debug

Enable or disable debug mode. Without an argument, it toggles the debug state. Optionally, you can include a state argument (`on` or `off`)

Syntax

`debug <on | off>`

clean load_balance_inactive_stap_queue

Use this command to manually clear an inactive S-TAP and its corresponding collector from the inactive S-TAPs queue in the load balancer.

Syntax

`clean load_balance_inactive_stap_queue <stapHost> <collectorName>`

delete scheduled-patch

To delete a patch installation request, use the **delete scheduled-patch** CLI command.

For more information about installing patches, see the **store system patch install** CLI command.

[delete ssl_gui_ciphers and restore ssl_gui_ciphers](#)

Use these commands to select and delete out-of-date GUI ciphers, and, if necessary, restore deleted ciphers.

Syntax

```
delete ssl_gui_ciphers
```

Guardium returns a list of ciphers. Specify the number of the cipher to delete. Use a comma to separate multiple cipher numbers.

Click q to quit without deleting any ciphers.

If you accidentally delete the wrong cipher, use restore ssl_gui_ciphers to restore it.

Restore command

```
restore ssl_gui_ciphers [ last | list ]
```

Where:

- last: Restores one or more last deleted ciphers.
- list: Restores all deleted ciphers.

Before you restore ciphers, Guardium warns that restoring the certificates can affect the connectivity of GUI and GIM-TLS. Make sure that when you restore deleted ciphers, the results that are returned are expected.

Show command

```
show ssl_gui_ciphers
```

For more information about supported ciphers, see [Cipher suites](#).

[delete unit type](#)

Use this command to clear one or more unit type attributes. Note that this command cannot clear all unit type attributes. For more information, see [store unit type](#).

Syntax

```
delete unit type [manager | standalone] [aggregated] [netinsp] [network routes static] [stap] [mainframe]
```

[eject](#)

This command dismounts and ejects the CD ROM, which is useful after you upgrade or reinstall the system, or after you install patches that were distributed on a CD ROM.

Syntax

```
eject
```

[export gim_bundle](#)

This command exports a selected S-TAP bundle that contains a custom K-TAP module from one GIM server to another.

Syntax

```
export gim_bundle <IP address or hostname>
```

IP address or hostname is the name of the machine to which you want to export the custom K-TAP module.

Note: You can run this command from any GIM appliance. Before you begin, make sure that the bundle you want to export is available on your current machine. When you run this command, a numbered list of all of the S-TAP bundles on your current machine that include a custom K-TAP module displays. To export an S-TAP bundle with a custom K-TAP module:

1. Run the **export gim_bundle** command.
2. Select the bundle that you want to export.
3. Guardium exports the bundle to the staging directory on the GIM appliance that you specified.
4. From the new GIM appliance, run the **grdapim_load_package** GuardAPI to upload the S-TAP bundle to your GIM appliance. For more information, see [gim_load_package](#).

[forward support email](#)

When the support-state option is enabled (which it is by default), this command sets the email address to receive system alerts.

Syntax

```
forward support_email to <email address>
```

Show command

```
show support-email
```

[import jproxy_files](#)

Use this command, along with **store jproxy_config ssh_key_file** to upload the GBDI SSH key file (in .pem format) and configure the SSH target host to communicate with GBDI. For more information, see [store jproxy_config ssh_key_file](#).

iptraf

IPTraf is a network statistics utility that is distributed with the underlying operating system. It gathers information such as TCP connection packet and byte counts, interface statistics and activity indicators, TCP/UDP traffic breakdowns, and LAN station packet and byte counts. For more information, see the IPTraf User Manual at the following location (it might also be available at other locations):

<http://iptraf.seul.org/2.7/manual.html>

Syntax

iptraf

license check

Indicates whether the installed license is valid. Use this command after you install a new product key.

Syntax

license check

license clear

Removes product licenses. After running this command, you will need to reapply base and append license keys and accept their terms and conditions. For more information about applying licenses, see [License keys](#) and [Install license keys](#).

Syntax

license clear

ping

Sends ICMP ping packets to a remote host. This command is useful for checking network connectivity. The value of host can be an IP address or host name.

Syntax

ping <host>

quit

Exits the command-line interface.

Syntax

quit

recover failed

Command to restore failed CSV/CEF/PDF transfer files, placing the files back into the export folder for another export attempt.

Syntax

recover failed [csv|cef|pdf]

register management

Registers the Guardium system for management by the specified central manager. The pre-registration configuration of this Guardium system is saved, and that configuration is restored later if the unit is unregistered.

Syntax

register management <manager ip> <port>

Parameters

manager ip is the IP address of the central manager.

port is the port number used by the central manager (usually 8443).

reset luks keys

Clears all stored tang keys in the Linux Unified Key Setup (LUKS) and removes all connections to the tang server.

Syntax:

reset luks keys

restart datastreams

Use this command to restart stopped AWS database activity-monitoring data streams. For more information, see [Cloud database service protection with data streams](#).

12.0 Syntax

restart datastreams

12.1 and later Syntax

```
restart datastreams [--yes]
```

Where --yes causes the command to run automatically.

restart gui

Restarts the IBM® Guardium Web interface. To optionally schedule a restart of the GUI once a day or once a week, use additional parameters. HH is hours 01-24. MM is minutes 01-60. W is the day of the week, 0-6, Sunday is 0. If HHMM is listed twice, only the last entry is used. The parameter clear deletes the scheduled time.

In order to restart the classifier and security assessments processes, run the **restart gui** command from the CLI (not from the GUI).

Running **restart GUI** from the GUI only restarts the web services. It is necessary to run the **restart GUI** command from the CLI to fully restart all processes, including Classifier and Security Assessments processes. It is necessary to run the **restart GUI** command from the CLI for each managed unit to restart the Classifier listener.

12.0 Syntax

```
restart gui [HHMM|HHMMW|clear]
```

12.1 and later Syntax

```
restart gui [HHMM|HHMMW|clear] [--yes]
```

Where --yes causes the command to run automatically.

restart rds_monitoring

Restart the AWS RDS monitor for Oracle. For more information, see [Cloud database service protection with native audit](#).

12.0 Syntax

```
restart rds_monitoring
```

12.1 and later Syntax

```
restart rds_monitoring [--yes]
```

Where --yes causes the command to run automatically.

restart sniffer_buffer_usage

Restarts the sniffer buffer.monitor.

12.0 Syntax

```
restart sniffer_buffer_usage
```

12.1 and later Syntax

```
restart sniffer_buffer_usage [--yes]
```

Where --yes causes the command to run automatically.

For more information about using **restart sniffer_buffer_usage**, see [Performance issue: buffer usage process not running](#).

restart stopped_services

Use this CLI command to restart services previously stopped with the **store auto_stop_services_when_full** CLI command.

12.0 Syntax

```
restart stopped_services
```

12.1 and later Syntax

```
restart stopped_services [--yes]
```

Where --yes causes the command to run automatically.

restart system

Reboots the Guardium system. The system will completely shut down and restart, which means that the cli session will be terminated.

12.0 Syntax

```
restart system
```

12.1 and later Syntax

```
restart system [--yes]
```

Where --yes causes the command to run automatically.

restart ticket_service

Restarts the external ticketing service. For more information, see [Configure an external ticketing system](#).

You can also stop and start the ticketing service from the CLI.

12.0 Syntax

```
restart ticket_service
```

12.1 and later Syntax

```
restart ticket_service --yes
```

Where --yes causes the command to run automatically.

restore rsyslog

Compares the current remotelog (rsyslog) on your system with an rsyslog that is restored from a CONFIG backup file, if one is available. You can then choose to override the existing rsyslog with the backed-up rsyslog.

Syntax

```
restore rsyslog
```

show buffer

This command displays a report of buffer use for the inspection engine process. If you are experiencing load problems, IBM Technical Support may ask you to run this command.

Syntax

```
show buffer <log | snif>
```

Examples

To display the buffer usage of the inspection engine process:

```
show buffer log
```

To display the buffer usage of the sniffer:

```
show buffer snif
```

show build

Displays build information for the installed software (build, release, snif version).

Syntax

```
show build
```

show load_balance_inactive_stap_queue

This command shows the list of inactive S-TAPs and corresponding collectors that have accumulated in the load balancer's inactive S-TAP queue.

Syntax

```
show load_balance_inactive_stap_queue
```

show network routes static

Permit the user to have only one IP address per appliance (through the primary interface) and direct traffic through different routers using static routing tables. List the current static routes, with IDs.

Syntax

```
show network routes static
```

Delete command

```
delete network routes static
```

show remotelog

Displays information about the rsyslog program that runs syslog. For information about adding and configuring remote logs, see the **store remotelog** commands, beginning with [store remotelog add](#).

Syntax

```
show remotelog <escape_control_characters_on_receive | host | max_message_size| status | test>
```

Where:

- **escape_control_characters_on_receive** - Displays the value of the rsyslog \$EscapeControlCharactersOnReceive directive.
- **host** - Displays the name of any remote hosts.
- **max_message_size** - Displays the value of the rsyslog \$MaxMessageSize directive.
- **status** - Displays the status of the rsyslog.
- **test** - Verifies the configuration of a configured rsyslog, as follows:
 - If the remote log is configured: The configuration displays. The test message sent to syslog targets the configured facility.priority. If the facility is ALL, then the message is sent using the **daemon** facility. If the priority is ALL, then the message is sent using **info**. You can verify that the messages are sent. To confirm, gather a tcpdump targeting the hosts, ports, and protocols and verify that rsyslog is transmitting the messages to the SIEM system. For more information, see [Facility and priority of syslog messages](#).
 - If a remote log is not configured, then a test message is sent to syslog without a specific facility or priority.

Syntax

```
show remotelog escape_control_characters_on_receive
show remotelog host
show remotelog max_message_size
show remotelog status
show remotelog test
```

Examples

```
show remotelog host
```

Sample output

```
Remote syslog is in non-encrypted mode.
Remote syslog format is default.
user.=warning    @@9.30.252.111
user.=alert      @@myhost.mycompany
user.=alert      @@myhost.mycompany
```

```
show remotelog status
```

```
show remotelog test
```

Sample output

```
show remotelog status test
The following receivers are configured
Messages will be written to syslog targeting these.
Please verify that the messages were received.
```

The tests could take several minutes

| Facility | Priority | Protocol | Host:port |
|----------|----------|----------|-------------------|
| daemon | info | TCP | 9.30.252.192:514 |
| user | info | UDP | 9.30.252.192:514 |
| user | alert | TCP | 9.30.252.192:5514 |

```
Sending message: daemon.info: Guardium test message
Sending message: user.info: Guardium test message
Sending message: user.alert: Guardium test message
```

```
Test message 'Guardium test message' successfully sent to syslog
```

```
Analyzing tcpdump. If a message is found in the tcpdump
output, but not in the syslog receiver, please consult your
administrator for the syslog receiver.
```

```
Message to 9.30.252.192:514 sent
Message to 9.30.252.192:514 sent
Message to 9.30.252.192:5514 sent
ok
```

show security policies

Displays the list of security policies.

Syntax

```
show security policies
```

show ticket update interval

View the interval for updating the status of records from external ticketing systems like Service Now. For more information, see [Configure an external ticketing system](#).

Set the value using **store ticket update interval <n>**.

Show command

```
show ticket update interval
```

show tls enabled

Show the versions of TLS that are enabled on the current machine. Both TLS 1.2 and TLS 1.3 can be enabled on the same machine.

For more information about TLS versions, see [Managing the TLS version](#).

start datastreams

Use this command to start existing AWS database activity-monitoring data streams. For more information, see [Cloud database service protection with data streams](#).

Syntax

```
start datastreams
```

start rds_monitoring

Start the AWS RDS monitor for Oracle. For more information, see [Cloud database service protection with native audit](#).

Syntax

```
start rds_monitoring
```

start ticket_service

Starts the external ticketing service. The ticketing service synchronizes external tickets (such as Service Now tickets) that are stored in local system. When the ticketing service is running, the synchronization runs once an hour. For more information, see [Configure an external ticketing system](#).

You can also stop or restart the ticketing service from the CLI.

Syntax

```
start ticket_service
```

stop datastreams

Use this command to stop running AWS database activity-monitoring data streams. For more information, see [Cloud database service protection with data streams](#).

Syntax

```
stop datastreams
```

stop gui

Stops the Web user interface.

Syntax

```
stop gui
```

stop rds_monitoring

Stop the AWS RDS monitor for Oracle. For more information, see [Cloud database service protection with native audit](#).

Syntax

```
stop rds_monitoring
```

stop system

Stops and powers down the appliance.

Syntax

```
stop system
```

stop ticket_service

Stops the external ticketing service. For more information, see [Configure an external ticketing system](#).

You can also start or restart the ticketing service from the CLI.

Syntax

```
start ticket_service
```

store aes_256_cbc_encryption

Use this command to set password encryption for the datasource to AES-256-CBC. You can run this command on a central manager or standalone machine to toggle the encryption cipher. If you run the command on a central manager, the encryption propagates to any managed units.

Note: The central manager and all managed units must be running Guardium 11.5 or later. If any managed units are running an earlier version, Guardium returns an error message.

Syntax

```
store aes_256_cbc_encryption [ on | off ]
```

Show command

```
show aes_256_cbc_encryption
```

store apply_user_hierarchy

Use this CLI command to apply user hierarchy to audit receiver.

If ON, the non-audit group receiver (the receiver other than the audit group receiver (normal or role) will only see audit results with a group IP beneath the receiver's hierarchy, including the receiver.

Syntax

```
store apply_user_hierarchy [ON | OFF]
```

Show command

```
show apply_user_hierarchy
```

store alert_timestamp_unit

Controls the timestamp unit for syslog alerts. Default is seconds.

Syntax

```
store alert_timestamp_unit [millisecond | second]
```

Show command

```
show alert_timestamp_unit
```

store alert_object_num_limit

Sets the maximum number of objects to show in the Alert log with the %%Object or %%objectType variables.

Syntax

```
store alert_object_num_limit <n>
```

Where *n* is a positive integer between 1 and 50. The default is 10.

Show command

```
show alert_object_num_limit
```

store alert_verb_num_limit

Sets the maximum number of SQL verbs to show in the Alert log. You can also set this parameter from the GuardAPI or REST API. For more information, see [modify_guard_param](#).

Syntax

```
store alert_verb_num_limit <n>
```

Where *n* is a positive integer between 1 and 50. The default is 10.

Show command

```
show alert_verb_num_limit
```

store allow_simulation

Enables (on) or disables (off) the ability to run the Policy Simulation on the appliance.

To run the simulation, the original traffic must be replayed through the rules engine (with the policy needing to be tested). This requires some of the original SQL on the appliance to be saved with their values. The enable or disable of allow_simulation instructs IBM Guardium to save or NOT save any SQL or values whatsoever.

Syntax

```
store allow_simulation [on|off]
```

Show command

```
show allow_simulation
```

store alp_throttle

Use this CLI to determine the amount of data logged by the Analyzer into the GDM_FLAT_LOG table.

The analyzer can lose packets in the analyzer circular queue for several different reasons, including the following:

- The incoming packet rate is too high.
- The parser is too slow for some complex or long SQL statements.

- The analyzer is too slow for some database packets.

Use `store alp_throttle` to choose how much data to log into the GDM_FLAT_LOG table.

Syntax

```
store alp_throttle <n>
```

Where *n* can be 0 or a positive integer.

- If *n* = 0 (the default), report without logging any SQL statements.
- If *n* is a positive integer, report and log every *n*th SQL statement in GDM_FLAT_LOG.

Examples

To report and log all SQL statements (100%):

```
store alp_throttle = 1
```

To report and log every 2nd SQL statement (50%):

```
store alp_throttle = 2
```

To report and log every 1000th SQL statement (0.1%):

```
store alp_throttle = 1000
```

store analyzer

This command sets the value of the timeout of the ignore session and sets the duration of the ignore session.

Ignore session: The current request and the remainder of the session will be ignored. This action does log a policy violation, but it stops the logging of constructs and will not test for policy violations of any type for the remainder of the session. This action might be useful if, for example, the database includes a test region, and there is no need to apply policy rules against that region of the database.

Syntax

```
store analyzer [ignore_sess_timeout | max_open_sess]
```

Show command

```
show analyzer
```

store auto_stop_services_when_full

When ON, stops internal services if the database exceeds the 90% full threshold.

Inspection Engine, Classification and other Collection-related services will stop. Also, Aggregation import/restore will not process any new files.

To remediate, use the various Support commands (support clean audit_task, support clean log_files, support clean DAM_data, support show large_files) to analyze and manually purge large tables.

Syntax

```
store auto_stop_services_when_full [ON | OFF]
```

Show command

```
show auto_stop_services_when_full
```

store connect oracle_parser

Use this command to connect and disconnect the Oracle parser from the DB2 parser. The default is OFF (disconnect).

Syntax

```
store connect oracle_parser [ON | OFF]
```

Show command

```
show connect oracle_parser
```

store csv_fetch_size

This command is used by the report REST service to control total number of records. Guardium reports can be downloaded in CSV file format.

`store csv_fetch_size` and `store csv_max_size` are GLOBAL_PROFILE parameters that can only be modified via CLI.

Note: `csv_max_size` requires a restart of the GUI for changes to take effect. `csv_fetch_size` does not require a restart.

Syntax

```
show csv_fetch_size <num>
```

Where *<num>* is a number greater than 0

Show command

```
store csv_fetch_size
```

store csv_max_size

This command controls the size of the CSV downloads that are retrieved when you click Download all records from the report export menu. The default value is 30,000.

Note: csv_max_size requires a restart of the GUI for changes to take effect.

Syntax

```
store csv_max_size <num>
```

Where <num> is a number greater than 0.

Show command

```
show csv_max_size
```

store cyberark config_failover

Use this command to configure standby CyberArk vault servers on your Guardium system.

Syntax

```
store cyberark config_failover
```

store cyberark install

Use this command to install CyberArk on your Guardium system.

Syntax

```
store cyberark install
```

You are prompted to enter the vault host name or IP address, vault user name and vault password.

Show command

Use the show command to verify if CyberArk is installed on your Guardium system.

```
show cyberark status
```

store cyberark service [start | stop]

Use this command to start or stop the CyberArk service on your Guardium system.

Syntax

```
store cyberark service start  
store cyberark service stop
```

store cyberark uninstall

Use this command to uninstall CyberArk from the Guardium system.

Before uninstalling, you must remove the reference to the Guardium system from the CyberArk vault server first. For more information, see [Uninstalling CyberArk](#).

Syntax

```
store cyberark uninstall
```

store cyberark upgrade_parameter

Before installing the CyberArk SDK upgrade patch on your Guardium system, run this command to enter the CyberArk upgrade parameters. The upgrade parameters are the CyberArk vault hostname or IP address, the vault username, and the vault password.

Syntax

```
store cyberark upgrade_parameter
```

Show command

```
show cyberark upgrade_parameter
```

store default_queue_size

Use this command to control the ADMINCONSOLE_PARAMETER.DEFAULT_QUEUE_SIZE configuration parameter. The default is 25. The range is 25-300.

The sniffer must be restarted after a change in value.

Syntax

```
store default_queue_size <N>, where N is the number in range of 25 to 300
```

Show command

```
show default_queue_size 25
```

store defrag

Use this command to restore defragmentation defaults, or to set the defragmentation size. After entering this command, you must issue the **restart inspection-core** command for the changes to take effect. The defrag is relevant only for network sniffing through SPAM or a TAP device.

Syntax

```
store defrag [default | size <s> interval <i> trigger <t> release <r>]
```

Where:

- default: Restore the default size.
- S: The packet size in bytes, up to a maximum of 217 (131072)
- I: The time interval
- T: The trigger level
- R: The release level specified as a number of seconds, up to a maximum of the 31st power of two (2147483648).

Show command

```
show defrag
```

Identify fragmented packets and attempt to reconstruct the packets before they get to the network sniffing process. Defrag is relevant only for network sniffing through SPAM or a TAP device.

store delayed_firewall_correlation

Use this CLI command to hold a user connection until the decryption correlation has taken place.

Syntax

```
store delayed_firewall_collection [on | off]
```

Show command

```
show delayed_firewall_correlation
```

store disk_space_reserved

Use this command to change the amount of disk space to reserve on a Guardium aggregator or collector. Reserving disk space allows you to customize the percentage of free space to preserve on the data partition.

12.0 Syntax

```
store disk_space_reserved [ custom <pct> | reset ]
```

12.1 and later Syntax

```
store disk_space_reserved [ custom <pct> | reset [-- yes ] ]
```

Where:

- **custom <pct>** - The percentage of available disk space to reserve, from 0 to 100.
- **reset** - Reset the amount of reserved disk space to the default.
- 12.1 and later --yes causes the command to reset automatically.

Note: The suggested (and default) reserved disk space is 25% for an aggregator and 50% for a collector. If you set the reserved disk space to less than the default, a warning message displays.

When you run **store disk_space_reserved reset** the reserved disk space is reset to the default percentage based on the type of the machine (25% for an aggregator, 50% for a collector).

Show command

```
show disk_space_reserved
```

store dump_data_for_forensics

This command dumps full SQL details into the local Kafka server for forensic and analysis purposes.

12.0 Syntax

```
store dump_data_for_forensics <ON | OFF>
```

12.1 and later Syntax

```
store dump_data_for_forensics <ON | OFF> [--yes]
```

Where --yes causes the command to run automatically.

Show command

```
show dump_data_for_forensics
```

Note: You can also set the dump SQL details behavior on or off from the GuardAPI [modify_guard_param](#) DUMP_DATA_FOR_FORENSICS parameter.

store encrypt_must_gather

Guardium collects certain data (must gather information) that IBM support uses if something goes wrong. This command determines whether must gather data is encrypted (on) or compressed, but not encrypted (off).

Syntax

```
store encrypt_must_gather <on | off>
```

Show command

```
show encrypt_must_gather
```

store full-bypass

This command is intended for emergency use only, when traffic is being unexpectedly blocked by the Guardium system. When on, all network traffic passes directly through the system, and is not seen by the Guardium system.

When using this command, you will be prompted for the admin user password.

Syntax

```
store full-bypass <on | off>
```

store gdm_analyzer_rule

Analyzer rules - Certain rules can be applied at the analyzer level. Examples of analyzer rules are: user-defined character sets, source program changes, and firewall watch or firewall unwatch modes. Rules applied at the analyzer level means decisions can be made at an earlier stage.

Note: When applying analyzer rules on source program changes, if the source program does not match the exact pattern, add .* at the end of the pattern to deal with the possibility that the source program has a trailing space (unseen by user).

Syntax

```
store gdm_analyzer_rule [active_flag | new ]
store gdm_analyzer_rule active_flag <id> <on|off>
```

Where <id> is the rule ID.

Show command

Use the CLI command, show gdm_analyzer_rule, to see a list of GDM analyzer rules.

```
show gdm_analyzer_rule
```

store gdm_analyzer_rule new

Use the Guardium CLI to add an analyzer rule for a direct regular expression to Mask UID Chain pattern.

Syntax

```
store gdm_analyzer_rule new
Enter rule description (optional):
Enter rule type (required):
```

Example

```
store gdm_analyzer_rule new
Please enter rule description: new rule 4
Rule type
 1. Change source program
 2. Set alternate character set
 3. Send verdict
 4. HADOOP exclude
 5. Define protocol and port
 6. Ignore session after packets
 7. Set empty Oracle DB user when login information is missed
 8. Force MS SQL login
 9. Transform string
Please select rule type (required): 9
Please enter pattern (required, regex string): (.*)(-ppassword)(.*)
Please enter format (required, regex string): \\\\1-p****\\\\3
Do you want to activate the rule now? (Yes/No)
Y
ok
```

store gdm_http_session_template

Use this CLI command to set the template for the HTTP session.

Usage

```
store gdm_http_session_template [activate] [add] [deactivate] [remove]
```

Show command

```
show gdm_http_session_template
```

Attempting to retrieve the template information. It may take time. Please wait.

Table 1. store gdm_http_session_template

| ID# | Active URL Regex | Session Regex | Username Regex | Login_Session Regex | Comment | Logout_Session_ID | Logout_URL_Regex |
|-----|------------------|---|--|--------------------------|---------------------------------|-------------------|------------------|
| 1 | 1 | Cookie.*PHPSESSID=([a-zA-Z0-9_-]{32}) | .*user_name=([a-zA-Z0-9_-]{1,16}) | Set-Cookie:.*PHPSESSID= | example of HTTP session deleted | | |
| 2 | 1 | Cookie.*PSJSESSIONID=([a-zA-Z0-9_-]{32}) | .*SignOnDefault=([a-zA-Z0-9_-]{1,16}) | | example of HTTP session | cmd=logout | |
| 3 | 1 | Cookie.*JSESSIONID=([a-zA-Z0-9_-]{32}) | .*username=([a-zA-Z0-9_-]{1,16}) | Set-Cookie:.*JSESSIONID= | example of HTTP session | | Logout.jsp |

store log external

Use this command to set file size, flush period, gdm error and state of the log external. This rule displays only if the following CLI command is executed:

```
store log external state on
```

Then log external shows up as a policy action.

CLI command to check the state:

```
show log external state
```

CLI command to enable and disable this action:

```
store log external state on/off
```

Usage

```
store log external [file_size] [flush_period] [gdm_error] [state]
```

Syntax

```
store log external gdm_error <state>
```

Where state is on or off. 'on' is to enable and 'off' is to disable.

```
store log external file_size <num>
```

Where <num> is the size of the file. Default is 4096 bytes.

```
store log external flush_period <num>
```

Where <num> is the flush period. Default is 60 seconds.

```
store log external state <state>
```

Where state is on or off. 'on' is to enable and 'off' is to disable.

Show command

```
show log external [file_size] [flush_period] [gdm_error] [state]
```

store monitor gdm_statistics

Use this CLI command to get information about the Unit Utilization. Default is 1 (run the script every hour).

Syntax

```
store monitor gdm_statistics
```

USAGE: store monitor gdm_statistics <hour>, where hour is a value from 0 to 24. Default value is 1, means to run the script every hour. Value 0, means not to run the script.

Show command

```
show monitor gdm_statistics
```

Disable command

```
Disable gdm_statistics monitor
```

store gui

Sets the TCP/IP port number on which the IBM Guardium appliance management interface accepts connections. The default is 8443.

n must be a value in the range of 1024 to 65535. Be sure to avoid the use of any port that is required or in use for another purpose.

Set session timeout: Sets the length of time (in seconds) with no activity before timeout. After the no-activity-timeout has been reached, it is necessary to log on again to Guardium. The default length is 900 seconds (15-minutes).

Enable or disable the Cross-site Request Forgery (CSRF) status. Trying to use certain web browser functions (for example, F5/CTRL-R/Refresh/Reload, Back/Forward) results in a 403 Permission Error message.

The new session timeout value will take effect only after the next GUI restart.

Syntax

```
store gui port <n>
store gui session_timeout <n>
store gui csrf_status [on | off]
```

Show command

Displays the GUI port number, state, session timeout (in seconds) and/or CSRF status.

```
show gui [port | state | all | session_timeout | csrf_status ]
```

store gui cache

Use this CLI command to turn web browser caching ON or OFF (Enable or Disable).

The response is:

```
The parameter has been changed.
Restarting gui
Changing to port 8443
Stopping.....
Safekeeping xregs
ok
```

The default setting for browser caching is enabled.

The act of changing the cache setting will automatically restart the Guardium web server.

For Firefox, you must clear the browser cache for the setting to take effect.

Syntax

```
store gui cache [ON | OFF]
```

Show command

```
show gui cache
```

store gui hsts_status

Use this CLI command to enable or disable the HSTS (HTTP Strict Transport Security Filter). This option is disabled by default on upgraded systems and is recommended to be turned on after valid certificates are installed. See the topic, How to install an appliance certificate to avoid a browser SSL certificate challenge, for further reference.

Syntax

```
store gui hsts_status [ on | off ]
```

Show command

```
show gui hsts_status
```

store gui xss_status

Use this CLI command to enable or disable the Cross-Site Scripting (XSS) status. This option is enabled by default on upgraded systems.

Syntax

```
store gui xss_status [ on | off ]
```

Show command

```
show gui xss_status
```

store installed security policy

Sets the security policy named **policy-name** as the installed security policy.

Syntax

```
store installed security policy <policy-name>
```

Show command

```
show installed security policy
```

store jproxy_config flush_at_size/store jproxy_config flush_timeout_sec

Use these commands to configure the streaming interval for transporting the JSON document data from Guardium to Guardium Big Data Intelligence (GBDI). Whenever Guardium hits either threshold, jProxy sends the data to GBDI. For more information, see [Big Data Intelligence with data streaming](#).

Syntax

```
store jproxy_config flush_at_size <bytes>
```

The default is 102400000.

```
store jproxy_config flush_timeout_sec <seconds>
```

The default is 60 seconds.

Show commands

```
show jproxy_config flush_at_size <bytes>
show jproxy_config flush_timeout_sec <seconds>
```

store jproxy_config ssh_key_file

Use this command, along with **import jproxy_files** to upload the GBDI SSH key file (in .pem format) and configure the SSH target host to communicate with GBDI. For more information, see [Big Data Intelligence with data streaming](#)

Syntax

```
import jproxy_files
store jproxy_config ssh_key_file <key_file_name>
```

- Use **import jproxy_files** to import the signed certificate (the SSH key file).
- Use **store jproxy_config ssh_key_file <key_file_name>** to store the SSH key file in the keystore.

store keep_psmls

Use this CLI command to retain the current layouts/profiles/portlets created by the users of the Guardium application. Set this CLI command to ON before an upgrade, and the psmls from the previous version will be retained.

Syntax

```
store keep_psmls [ON | OFF]
```

Show command

```
show keep_psmls
```

store ldap-mapping

Store LDAP-mapping parameters - allow a custom mapping for the LDAP server schema. This command permits customized mapping to the LDAP server schema for email, firstname and lastname attributes. The paging parameter is used to facilitate transfer between any LDAP server type (Active Directory, Novell Directory, Open LDAP, Sun One Directory, Tivoli® Directory). If the paging parameter is set to on, but paging is not supported by the server, the search is performed without paging.

Example for paging. If the CLI command, **ldap-mapping paging** is set to ON, then Microsoft Active Directory will download the maximum number users defined under the limit value on the LDAP Import configuration screen. If CLI command, **ldap-mapping paging** is set to OFF, then Active Directory will download up to only 1000 users no matter what the limit value is set to. All other LDAP server configurations must use the CLI command, **ldap-mapping paging off** in order to download users up to the set limit value.

Note: Each time you change the CLI ldap-mapping attributes you also need to select Override Existing Changes on the LDAP Import configuration screen in IBM Guardium GUI before updating. This action must occur each time you change the CLI ldap-mapping email, firstname or lastname attributes and import LDAP users.

Show commands

```
show ldap-mapping [email] [firstname][lastname] <name>
show ldap-mapping paging ON|OFF
```

A GUI restart of the CLI is required for new parameters to take effect.

Examples

```
store ldap-mapping firstname name
store ldap-mapping lastname sn
store ldap-mapping email mail
store ldap-mapping paging on
```

If the attributes are written as follows, the mapping process will use the first attribute it finds. If this is not what you want, use one of the examples to map to specific attributes.

- Values for firstname attribute: gn,givenName,name
- Values for lastname: attribute: sn,surname,name
- Values for email attribute: userPrincipalName,mail,email,emailAddress,pkcs9email,rfc822Mailbox
- Values for paging: on, off

store license

This command applies a new license key to the appliance.

A license key may be of one of two kinds: override type or append type; an override type replaces the currently installed license while the append type license will be appended to the currently installed license. Append-type licenses can only add functionality; new functions may be enabled and when relevant - updates expiration dates, the remaining number of scans, the number of datasources, or might replace certain numeric fields in the license, such as the number of managed units.

Syntax

```
store license
```

Example

When using the **store license** command, you are prompted to paste the new product key:

```
CLI> store license
Please paste the string received from customer services. Then press <ENTER> to continue.

Copy and paste the new product key at the cursor location, and then press Enter. The product key
contains no line breaks or white space characters, and it always ends with (and includes) a trailing
equal sign. A series of messages will display, ending with:
>We recommend that the machine be rebooted at the earliest opportunity in order to complete the
license updating process.
ok
CLI>
Run the restart gui command at this time.
```

Show command

```
show license
```

Shows details about the license for this appliance, as follows:

- License - A single license that includes the base license merged with information from any older licenses and append licenses. For central managers, this license key is sent to any associated managed units when the managed unit is registered or the system is refreshed.
- Number of Licenses - Specifies the number of managed units that can be associated with a central manager. This value cannot be changed after the license is installed.
- Metering - If this appliance has a metered license, then you can run only a certain number of vulnerability assessment scans. A value of -1 means there is no limit. For a metered license, Guardium checks this value each time you run a security assessment or classifier process. The process runs only if the number of datasources in the security assessment or classifier is less than or equal to the metering value. When a process runs, the metering value is updated by subtracting the number of datasources from the metering.
- Number of Datasources - The maximum number of datasources for which the appliance has license for. A value of -1 means there is no limit. This value cannot be changed after license installation. If your site has a limited license, the value is decremented each time you add or import a datasource. A datasource, for this purpose, is a database server that you add either from the Datasource Definition page of the Guardium UI, by using the **create_datasource** GRDAPI command.
- Valid until - The expiration date for this license.
- Licensed Applications - The Guardium applications that this appliance can access under this license.
- Licensed Product Types - The Guardium add-on products that this appliance can access under this license.

store log classifier level

Sets the debugging level for the classifier, to one of the values shown.

Syntax

```
store log classifier level TRACE|DEBUG|INFO|WARN|ERROR|FATAL
```

Show command

```
show log classifier level
```

store log exception sql

When **on**, logs the entire SQL command when logging exceptions.

Syntax

```
store log exception sql <on | off>
```

Show command

```
show log exception sql
```

store log_general_response_length

Use this CLI to enable or disable logging the response length. When enabled, controls whether the sniffer logs the response length for every SQL instance.

store log_general_response_length is disabled by default. Enabling response length logging can impact sniffer performance.

Syntax

```
store log_general_response_length [ enable | disable ]
```

Where:

- **enable** - Always log the response length. The responseLength value is logged for all entities.
- **disable** - Do not log the response length (default).

Show command

```
show log_general_response_length
```

store log object_join_info

Sets the logging of object_join.

A join table is a way of implementing many-to-many relationships. Use join entity to join tables in a SELECT SQL statement.

Syntax

```
store log object_join_info [ on | off]
```

Show command

```
show log object_join_info
```

store log object_join_info

Sets the logging of object_join.

A join table is a way of implementing many-to-many relationships. Use join entity to join tables in a SELECT SQL statement.

Syntax

```
store log object_join_info [ on | off]
```

Show command

```
show log object_join_info
```

store log session_info

This command enables or disables storing sniffer log session information.

Syntax

```
store log session_info [ on | off]
```

Show command

```
show log session_info
```

store log sql parser_errors

Sets the logging of syntactically wrong SQL commands.

Syntax

```
store log sql parser_errors [on|off]
```

Note: A restart of the inspection engine is required after the store command is issued to apply change.

Show command

```
show log sql parser_errors
```

store logger_data_destination_config

Use the following CLI commands to optionally configure information for Guardium Big Data Intelligence (GBDI) data streaming such as logger destination, Mongo client authentication (username, auth, database, and mechanism).

For more information, see [Big Data Intelligence with data streaming](#).

- `store logger_data_destination_config type <database type>`
 - `store logger_data_destination_config database_name <db name>`
 - `store logger_data_destination_config destination [hostname | port] <value>`
 - `store logger_data_destination_config [auth_username | auth_database_name | mechanism] <value>`
 - `store logger_data_destination_config data <collection type> [on|off]`
- Where the collection types are:
- session
 - instance
 - full_sql
 - policy_violations
 - exception

Show command

```
show logger_data_destination_config <parameter>
```

store logging granularity

Sets the logging granularity to the specified number of minutes. You must use one of the minute values shown in the syntax. The default is 60.

Syntax

```
store logging granularity <1, 2, 5, 10, 15, 30 or 60>
```

Show command

```
show logging granularity
```

store max_audit_reporting

Displays the audit report threshold in days. The default is 32. When defining reports in audit process, the number of days of the report (defined by the FROM-TO fields) should not exceed a certain threshold (one month by default). For more information, see [Audit processing notes](#).

Syntax

```
store max_audit_reporting <days>
```

Show command

```
show max_audit_reporting
```

store max_result_set_packet_size

Store the max_result_set_packet_size, default value is 32 (size is between 1 and 65535) and aids in tuning the inspection engine when observing returned data. This command sets the limitation for packet size in response. This parameter works for any type of database. If the value is beyond the defined threshold, the analyzer will not retrieve data to calculate records affected value.

Syntax

```
store max_result_set_packet_size <size>
```

Show command

```
show max_result_set_packet_size
```

store max_result_set_size

Store the max_result_set_size, default value is 100 (size is between 1 and 65535) and aids in tuning the inspection engine when observing returned data. This command sets the limitation for total result set size. This parameter works for any type of database. If the value is beyond the defined threshold, the analyzer will not retrieve data to calculate records affected value.

Syntax

```
store max_result_set_size <size>
```

Show command

```
show max_result_set_size
```

store max_tds_response_packets

Store the max_tds_response_packets, default value is 5 (size is between 1 and 65535) and aids in tuning the inspection engine when observing returned data. This command sets the limitation for number of packets in response. This parameter works for MS SQL only. If the value is beyond the defined threshold, the analyzer will not retrieve data to calculate records affected value.

Syntax

```
store max_tds_response_packets <size>
```

Note: max_tds_response_packets (Tabular Data Stream) is only applicable for MS SQL Server and Sybase.

Show command

```
show max_tds_response_packets
```

store maximum query duration

Sets the maximum number of seconds for a query to the value specified by **n**. The default is 180. We recommend that you **do not** set this value greater than the default, because doing so increases the chances of overloading the system with query processing. This value can also be set from the Running Status Monitor panel on the administrator portal.

Syntax

```
store maximum query duration <n>
```

Show command

```
show maximum query duration
```

store monitor

Use the store monitor buffer CLI command to

Syntax

```
store monitor [buffer | custom_db_usage [state <hour>] | gdm_statistics <hour> ]
```

Where:

- buffer - Set the interval of how often to run the script that retrieves the information shown in the Buffer Usage Monitor report of the IBM Guardium Monitor tab.
- custom_db_usage [state][hour] - Set the state and specify a time to run this job.
When state = *on*, specify the hour (0 - 23) to run.
- gdm_statistics <hour> - Get information about the Unit Utilization, where *hour* is a value from 0 to 24. Default = 1 (run the script every hour).

Show commands

```
show monitor buffer
show monitor custom_db_usage
show monitor gdm_statistics
```

store mysql_utf8mb4

Enable support for 4-byte UTF-8 encoding (utf8mb4).

This command modifies Guardium sniffer processes and internal databases to correctly capture and store 4-byte UTF-8 characters. Enabling utf8mb4 may be useful if datasources in your environment contain 4-byte characters, for example as used for Chinese, Japanese, and Korean ideographs.

Observe the following when using this command:

- The additional processing required to capture and store 4-byte characters will negatively impact the performance of your Guardium system. For this reason, do not enable utf8mb4 unless you require 4-byte character support in your environment.
- If support for 4-byte UTF-8 encoding is required in an aggregated or centrally managed environment, utf8mb4 should be enabled on all Guardium systems in the environment. Enabling utf8mb4 on only some systems in the environment may create problems, such as failed aggregation or incorrectly displayed reports.
- Data collected or aggregated before enabling utf8mb4 will still be available and function correctly after enabling utf8mb4.

CAUTION:

Once 4-byte UTF-8 support has been enabled using the **store mysql_utf8mb4** command, the change cannot be undone or reversed. After enabling utf8mb on a Guardium system, the only way to remove support for 4-byte UTF-8 characters is to completely rebuild the system.

Important: To ensure that multi-bytes are represented correctly on your Guardium system, you must restart sniffer as soon as you enable mysql_utf8mb4.

12.0 Syntax

```
store mysql_utf8mb4
```

Syntax12.1 and later Syntax

```
store mysql_utf8mb4 [--yes]
```

Where --yes causes the command to run automatically.

Show command

```
show mysql_utf8mb4
```

Examples

```
> show mysql_utf8mb4
```

mysql configuration NOT set with UTF8MB4.
ok

```
>store mysql_utf8mb4
```

Attempting to change the mysql config file. It may take time. Please wait.
Start to modify mysql config file
Restarting mysql
Mysql has been restarted. Please exit CLI and log back on.
The parameter IS_UTF8MB4 has been changed to 1.

```
> show mysql_utf8mb4
```

mysql configuration set with UTF8MB4.
ok

store packet max-size

Limit the maximum size of packets from the sniffer.

Syntax

```
store packet max-size 1536
```

Show command

```
show packet max-size
```

store pdf-config

Use this command to change the font size and orientation of the PDF image body content (excluding header/footer).

Size unit ranges from 1 (smallest) to 10 (largest) with default value of 6.

Orientation unit is 1 (for landscape orientation) or 2 (for portrait). The default value is 1.

The change takes effect immediately after typing the CLI command and pressing the Enter key.

Syntax

```
store pdf-config [ orientation | size ]
```

Show command

```
show pdf-config [ orientation | size ]
```

store pdf-config multilanguage_support

There are different static PDF generator config files for English (Used on English version) and language C/J (Used on Chinese/Japanese). Use this CLI command to define the fonts in the PDF generator. Default is English. Multilanguage is language C/J.

Syntax

```
CLI> store pdf-config multilanguage_support
```

Current setting is Default

```
1 Default  
2 Multi-language  
Please select the option (1,2, or q to quit)
```

Show command

```
show pdf-config multilanguage_support
```

store populate_from_query_maxrecs

Sets the maximum number of records that can be used to populate groups and aliases from a query.

Use caution when setting a maximum records value via this CLI command. Setting it too high may result in incomplete populate group from query processes. The maximum threshold is dynamic and dependent on the system load and memory utilization. The default value is 20,000 records. The maximum configurable value is 200,000 records.

Syntax

```
store populate_from_query_maxrecs 100000
```

Show command

```
show populate_from_query_maxrecs
```

store product gid

Sets the stored unique product <n> GID value.

Syntax

```
store product gid <n>
```

Show command

```
show product gid
```

store purge object

Sets the age (in days) at which non-essential objects will be purged. Use the **show purge objects age** command to display a table showing the index, object name, and age for each object type for which a purge age is maintained. Then use the appropriate index from that table in the command to set the purge age.

Note: The value of number of days will be set to the default (90 days) when the unit type changes between managed unit/Manager/standalone unit.

Syntax

```
store purge object age <index> <days>
```

Show command

```
show purge object age
```

Example

Assume you want to keep an Event Log for 30 days. First issue the **show purge objects age** command to determine the index (do not use the table; your list may be different). Then enter the **store purge object** command.

For example:

```
>show purge objects age
```

```
Index Name, Age  
... purge objects
```

```
>store purge object age 2 30
```

store quartz_thread_num

This CLI command is for use by Technical Support.

The Java™ Virtual Machine allows the application to have multiple threads. Thread is a piece of the program execution.

Use the **store quartz_thread_num** CLI command to set the number of threads that can run at the same time.

Use this command to ease conflict between too many threads running at the same time.

The **show quartz_thread_num** CLI command displays the number of Quartz scheduler threads that run at the same time.

12.0 Syntax

```
store quartz_thread_num <number>
```

12.1 and later Syntax

```
store quartz_thread_num [number [-yes]]
```

Where --yes causes the command to run automatically.
Where number is in range 3 to 15. Default value = 5.

Show command

```
show quartz_thread_num  
org.quartz.threadPool.threadCount= 5
```

store remotelog add

Controls the use of remote logging. In addition to system messages, statistical alerts and policy rule violation messages can be written to syslog. For each host and port combination, you can direct messages from the syslog to a remote host. This command works with any syslog implementation that supports TCP or UDP protocol.

If you enable remote logging, be sure that the receiving host can accept the log information.

Syntax

```
store remotelog add <encrypted | non_encrypted> <facility.priority> <host[:port]> <protocol> [format]
```

Where:

- **<encrypted | non_encrypted>** - Specify whether the connection to the remote host is encrypted. Guardium suggests that you encrypt all communications to a remote syslog server.

Note: To add an encrypted log, you must provide a signed certificate. For more information, see [Encrypting syslog](#).

- **facility** - Required. The service routed to the remote logger. To see the available facilities, enter **store remotelog add encrypted ?** in the CLI.
- **priority** - Required. The log priority, which can be:

- **alert** - Guardium severity code HIGH
- **all**
- **crit**
- **debug**
- **emerg**
- **err** - Guardium severity code MED
- **info** - Guardium severity code INFO
- **notice**
- **warning** - Guardium severity code LOW

Note: Both facility and priority are required, in the format **facility.priority**.

- **host** (required) and **port** - The remote host name or IP address and optional port to send syslog messages. The default port is 514.

- **protocol** - Required. The protocol to use to connect to the remote host. Protocol can be either:

- **tcp**
- **udp**

Note: Only TCP supports encrypted connections to the remote host.

- **format** - Some SIEM products process IETF RFC 5424 style syslog messages better than the default messages. This parameter changes the syslog format for this remote logger only to one of the following options:
 - **default** - rsyslog default format.
 - **rfc5424** - rsyslog RFC 5424 format.

Note: To use RFC 5425 format, the syslog receiver must be configured to accept RFC 5424 format. Otherwise, it receives the log in the default format.

Examples

```
cli> store remotelog add encrypted user.info 9.30.252.111 tcp  
  
cli> store remotelog add non_encrypted user.warning myhost.mycompany.com tcp  
tcp forwarder to myhost.mycompany.com added to rsyslog configuration:  
user.=warning @myhost.mycompany.com  
Restarting remote logger...  
Remote logger restarted successfully  
ok  
cli> store remotelog clear myhost.mycompany.com  
Remote logger configuration updated.  
Restarting remote logger...  
Remote logger restarted successfully
```

store remotelog clear

Use this command to clear the specified facility.priority combination from the list of messages to send to the specified host.

Syntax

```
store remotelog clear host
```

Example

```
cli> store remotelog clear myhost.mycompany.com  
Remote logger configuration updated.  
Restarting remote logger...  
Remote logger restarted successfully
```

store remotelog escape_control_characters_on_receive

Use this command to escape the control characters if your system mangles messages that include control characters. The default is on (escape control characters).

Syntax

```
store remotelog escape_control_characters_on_receive <on|off>
```

Run **restart remotelog** to apply the new configuration.

store remotelog format

Sets the default syslog format in the rsyslog configuration (in the global directive **\$Undoable-in-transactional**).

Some SIEM products process IETF RFC 5424 style syslog messages better than the default messages. In that case, change the format to **rfc5424**.

Note: The **store remotelog format** command permanently changes the default format.

- **default** - rsyslog default format.
- **rfc5424** - rsyslog RFC 5424 format.

Note: To use RFC 5425 format, the syslog receiver must be configured to accept RFC 5424 format. Otherwise, it receives the log in the default format.

Run **restart remotelog** to apply the new configuration.

store remotelog max_message_size

Use this command to set the maximum message size from 5k to 64k. Specify the maximum message size with a single number, as follows:

- 1 = 5k
- 2 = 10k
- 3 = 15k
- 4 = 20k
- 5 = 32k
- 6 = 64k

Syntax

```
store remotelog max_message_size <1|2|3|4|5|6>
```

Run **restart remotelog** to apply the new configuration.

Show command

Use this command to display the current value of the **\$MaxMessageSize** parameter.

Configuring remotelog receivers

To configure a receiving system to accept remote logging, edit **/etc/sysconfig/syslog** on the system to include the **-r** option. For example:

```
SYSLOGD_OPTIONS=-r -m 0
```

Then restart the syslog:

```
/etc/init.d/syslog restart
```

The standard syslog file in Linux® is named:

```
/var/log/messages
```

Notes:

- To send the encrypted remote log message to the server, the rsyslog configuration in the server needs to accept encrypted messages.
- TCP protocol is required to use the encrypted setting on client and server.
- If you change from one mode to another, you need to modify the configuration file to sync with the designated mode and restart the remote service.

Encrypting syslog

Alerts and other messages can be forwarded to a remote syslog receiver, such as a SIEM system. This message traffic can be encrypted from the collector or aggregator to the remote syslog receiver.

Note: Encryption only works in TCP mode. By default, syslog forwarding uses UDP, so if encryption is required, specify TCP.

You need the certificate used by the remote syslog receiver. Store that certificate on the Guardium system.

To add an encrypted remote log:

1. Have the public certificate available from a CA (Certificate Authority) such as Verisign, Thwate, or in-house.
2. Log into the CLI on the individual Guardium system from which to send the encrypted syslog. Before you execute the command, obtain the appropriate certificate (in PEM format) from the CA, and copy the certificate, including the Begin and End lines, to your clipboard.
3. Enter the following CLI command:

```
store remotelog add encrypted user.all <remote host IP address>:<remote host port number> tcp
```

4. The following instructions display:

```
Please paste your CA certificate, in PEM format. Include the BEGIN and END lines, and then press CTRL-D.
```

- Paste the PEM-format certificate to the command line, then press **CTRL-D**. Guardium stores the input as **/etc/pki/rsyslog/ca.pem**.
- Guardium returns a message informing you of the success or failure of the store operation.
- If successful, Guardium can send encrypted traffic to the remote system with the correct key.

5. Repeat the procedure for each collector and aggregator that is sending syslog traffic to the encrypted host.

store s2c

Sets several configurable parameters for ADMINCONSOLE. These parameters are used for throttling server-to-client (S2C) traffic.

Note: Use this CLI command only when directed by IBM Guardium Technical Services.

Minimum and maximum values:

- ANALYZER_S2C_IGNORE = {0,1,2,3}
- MAX_S2C_VELOCITY (K bytes/sec) - number >=0 and <= 2147483647
- MAX_S2C_INTERVAL (sec) - number >=1 and <= 2147483647

See also the CLI command Store Throttle.

Syntax

```
store s2c
```

USAGE: store s2c ignore I maxrate M maxinterval T where 0<=I<=3 (level), 0<=M<=2147483647 (K/sec), and 1<=T<=2147483647 (seconds) OR store throttle default.

For example:

```
>store s2c ignore 3 maxrate 300 maxinterval 5007
```

The new configuration will take effect after you run the **restart inspection-core**,CLI command.

Show command

```
show s2c
```

Throttle S2C parameters (defaults):

```
Ignore:    0  
Max rate: 999999  
Max interval: 30
```

ANALYZER_S2C_IGNORE (0,1,2,3) - Switch s2c throttling mechanisms on/off based on scenarios. This flag is based on bits. 0 = the s2c throttling mechanism is OFF. 1 = turns on the function described in scenario 1, 2 = turns on the function described by scenario 2. 3 = turns both on.

MAX_S2C_VELOCITY - maximal rate (K bytes/sec). If this rate is exceeded, then analyzer should send CLI commands, ignore session, or ignore session reply, request to S-TAP® or sniffer.

MAX_S2C_INTERVAL - time interval in seconds (default 30 sec.) between possible CLI commands, ignore session, or ignore session reply, requests.

Scenario 1

The sniffer starts to receive traffic from S-TAP or network in the middle of large query. Since all incoming packets are DB server responses, no new session will be created by the analyzer and therefore no information will be sent to logger and rules engine. This type of traffic is useless for the sniffer. From the other side, this type of traffic can create additional S-TAP and sniffer loads.

A throttling mechanism helps to decrease S-TAP and network sniffer load by sending an ignore session message from the analyzer, if the S2C velocity is greater than MAX_S2C_VELOCITY. If, for some reason, S-TAP or network sniffer were not affected, then the analyzer sends ignore session request again after MAX_S2C_INTERVAL seconds. In order to switch this throttling mechanism on, set ANALYZER_S2C_IGNORE flag to 1.

Scenario 2

If the incoming traffic has a high S2C rate (>MAX_S2C_VELOCITY), then a throttling mechanism sends a ignore session reply request to S-TAP for local database connections in the case when S2C velocity is greater than MAX_S2C_VELOCITY. If from some reason S-TAP was not affected, then analyzer will send the ignore session reply request again after MAX_S2C_INTERVAL seconds. In order to switch this throttling mechanism on, set ANALYZER_S2C_IGNORE flag to 2.

store save_result_max_size

This CLI command modifies the GLOBAL_PROFILE field SAVE_RESULT_MAX_SIZE to set the amount of data in reports that are generated from the GUI that reflect the maximum number of result records in the reports.

Syntax

```
store save_result_max_size <num>
```

Where <num> is a number greater than 0.

Show command

```
show save_result_max_size
```

store sender_encoding

Use this CLI command to encode outgoing messages (email and SNMP traps) in different encoding schemes, where previously everything is encoded in UTF8.

For example, a Guardium customer wanted to encode all of the outgoing SNMP messages in SJIS - an alternative Japanese encoding.

Note: If the conversion fails, for either reason (a) the encoding scheme specified is invalid, or (b) the characters to be encoded can not be represented in the requested encoding scheme, then the message will be sent using UTF8, which is the default encoding scheme.

Syntax

```
store sender_encoding <str>,
```

where str is the encoding with maximum length 16

Show command

```
show sender_encoding
```

store set_informix_driver_property

Use this command to set the connection property IFX_USE_STRENC=true on all Informix® datasources.

12.0 Syntax

```
store set_informix_driver_property
```

12.1 and later Syntax

```
store set_informix_driver_property [--yes]
```

Where --yes causes the command to run automatically.

store set_partitions_for_queries

Use this CLI command to enable or disable partition selection on queries.

Syntax

```
store set_partitions_for_queries <on|off>
```

store skip_extrusion_on_sql_access_rule_match

Use this CLI to control extrusion rule actions for data security policy extrusion rule actions when the SQL access rule matches.

For more information, see [Logging or ignoring rule actions](#)

Syntax

```
store skip_extrusion_on_sql_access_rule_match [n]
```

Where n is one of the following values:

- 0 - Default. Do not skip extrusion rule actions.
- 1 - Skip all relevant extrusion rule actions.
- 2 - Skip only duplicate extrusion rule action.

Show command

```
show skip_extrusion_on_sql_access_rule_match
```

show snif_alert_only_syslog_with_subject

Use this command to determine whether the subject of alerts displays in the syslog. Set to OFF to hide the subject of alert messages. The default is ON, which displays the alert subject in the syslog.

Syntax

```
store snif_alert_only_syslog_with_subject on|off
```

Show command

```
show snif_alert_only_syslog_with_subject
```

store snif_double_quote_literal

Use this command to control whether the sniffer handles double-quoted strings as literals and replaces them with question marks when generating masked SQL. By default, the sniffer assumes that double-quoted strings are literals and masks accordingly. The setting is available for several database types. Upon running the command, you are asked to select the database type from a list and define whether quoted strings are treated as literals. Use **restart inspection-core** to restart the inspection engine core after changing **snif_double_quote_literal** settings.

Example

```
> store snif_double_quote_literal
This command controls whether or not snif will consider double quoted strings literals, and replace them
with question marks when generating masked sql.
USAGE: store snif_double_quote_literal
```

DB type:

1. MySQL
2. MemSql
3. MsSql
4. Sybase

```
5. Informix
0. Quit

Please select DB type to modify (required) 1

Consider double quoted strings literals?
(y/n)? n
The parameter has been changed.
Please restart the inspection core for this change to take effect:
restart inspection-core
ok
```

Show command

```
show snif_double_quote_literal
```

Example of show command

```
> show snif_double_quote_literal
Database types in which snif considers double quoted strings as literals
```

```
Mysql: No (default Yes)
MemSql: Yes (default Yes)
MsSql: Yes (default Yes)
Sybase: Yes (default Yes)
Informix: No (default No)
ok
```

[store snif_log_level](#)

Use this command to set the logging level for the sniffer.

Syntax

```
store snif_log_level [TRACE | DEBUG | DEFAULT]
```

Where DEFAULT is the default log level, INFO.

Show command

```
show snif_log_level
```

[store snif_logger_destination_type](#)

Use this command to control the sniffer logger destination for Guardium Big Data Intelligence (GBDI) data streaming.

Syntax

```
store snif_logger_destination_type [LOCAL | REMOTE]
```

- LOCAL (default) sets the logger destination to the local database on the Guardium collector.
- REMOTE sets the logger destination to the intermediate database used by GBDI.

For more information, see [Big Data Intelligence with data streaming](#).

[store snif_mask_sql_value](#)

Use this command to mask SQL values that are logged when a SQL exception occurs.

Note: If the SQL string contains a syntax error, only literals (that is, values enclosed in single quotation marks) are masked in the GDM_EXCEPTION table. For example, if the SQL string contains a syntax error, then the following masking rules apply:

'literal123' is a literal, as shown by the single quotation marks, and is masked.

`identifier123` is an identifier, and displays in the table in clear text.

Syntax

```
store snif_mask_sql_value on|off
```

Show command

```
show snif_mask_sql_value
```

[store snif_db2z_alert_use_client_ip_for_host_name](#)

For Db2 z/OS systems only, use this command to enable using the client IP address as the host name for Alert messages. When enabled, the %%clientHostName variable displays the host IP address.

Syntax

```
store snif_db2z_alert_use_client_ip_for_host_name [on|off]
```

Note: For this command to take effect, you must also restart the inspection engine by calling the [restart inspection-engine](#) command.

Show command

```
show snif_db2z_alert_use_client_ip_for_host_name
```

[store snif_max_db2z_bind_variable_value_size](#)

For Db2 z/OS systems only, use this command to control the length, in KB, of bind variable values. The default length is 2 KB (2047 characters). The maximum length is 4096 KB.

Syntax

```
store snif_max_db2z_bind_variable_value_size <n>
```

Where <n> is a number between 2 and 4096, which is the maximum length of the bind variable values in KB.

Show command

```
show snif_max_db2z_bind_variable_value_size
```

store snif_use_feed_analyzer_thread

When Guardium processes S-TAPs on multiple ports, you can encounter issues in which multiple S-TAPs use the same queue and buffer. Specifically, if your site uses ports 16016 or 16018 (for UNIX S-TAPs) and ports 16022 (feed protocol) or 16023 (encrypted S-TAP TLS) the S-TAPs default to a shared queue, which can lead to unexpected issues.

The **store snif_use_feed_analyzer_thread** command allows you to have sniffer use a separate internal queue for these S-TAPs.

The default for **store snif_use_feed_analyzer_thread** is *OFF*. If you expect traffic on both ports (that is 16016 or 16018 and 16021 or 16022), set **store snif_use_feed_analyzer_thread** to *ON* before the S-TAPs start.

In addition, if the sniffer detects traffic from both ports, sniffer sets the parameter to *ON*, causing sniffer to use separate queues after the next restart.

Syntax

```
store snif_use_feed_analyzer_thread [ON | OFF]
```

Note: For this command to take effect, you must also restart the inspection engine by calling the [restart inspection-engine](#) command.

Show command

```
show snif_use_feed_analyzer_thread
```

store ssl_configuration

Use this command to specify the ciphers used by the Guardium sniffer for your operating system.

Syntax

```
store ssl_configuration
```

When you run this command, Guardium returns a list of ciphers and indicates whether your system uses each cipher (indicated by an x, for example. [x]). Specify the number of the cipher (or ciphers) to toggle on or off. Use a comma to separate multiple cipher numbers.

Click q to quit without making changes.

When you are done specifying the ciphers that you want, click s to save your changes, which restarts the sniffer to load the selected ciphers.

Show command

```
show ssl_configuration
```

For more information about supported ciphers, see [Cipher suites](#).

store stop approval

Use this function to block unauthorized S-TAPs from connecting to the Guardium appliance.

If ON, then S-TAPs can not connect until they are specifically approved.

If an unapproved S-TAP connects, it is immediately disconnected until the specific authorization of the IP Address of that S-TAP.

A pre-defined report for approved clients, Approved TAP clients, is available on the Daily Monitor tab.

Note:

A valid IP address is required, not the host name.

The CLI command, **store stap approval**, does not work within an environment where there is an IP load balancer.

Within a central manager environment, after adding the IPs to approved S-TAPs, there is a wait time associated with synchronization that might take up to an hour. After synchronization is complete the approved S-TAP status will appear green in GUI.

Syntax

```
store stap approval ON | OFF
```

Show command

```
show stap approval
```

GuardAPI command

```
grdapic store_stap_approval  
The new configuration takes effect after running the CLI command, restart inspection-core.
```

store stap certificate

Stores a certificate from the S-TAP host (usually a database server), on the IBM Guardium appliance. This command functions exactly like the store certificate console command, described later.

Syntax

```
store stap certificate
```

You will be prompted as follows:

Please paste your new server certificate, in PEM format.

Include the BEGIN and END lines, then press CTRL-D.

If you have not done so already, copy the server certificate to your clipboard. Paste the PEM-format certificate to the command line, then press CRTL-D. You will be informed of the success or failure of the store operation.

When you are done, use the **restart gui** command to restart the IBM Guardium GUI.

store stap network_latency

S-TAP verification is a feature by which customers can verify if a S-TAP is monitoring database traffic or not. The verification feature is affected by the customer's network traffic/latency. Since latency is different for each customer, there is a need for a way to list and change the default value that the verification feature uses.

Syntax

```
store stap network_latency
```

USAGE: store stap network_latency <N>

where N is the number greater than 0 seconds.

The default value is 5 seconds.

If the number goes higher the S-TAP verification process will become slower.

Show command

```
show stap network_latency
```

store storage-system

store storage-system

Adds or deletes a storage system type for archiving or system backup.

Syntax

```
store storage-system <NETWORK | Amazon_S3 | Centera | IBMCloud | IBMcos | NFS | TSM> <backup | archive> <on | off>
```

Show command

```
show storage-system
```

Restriction: External storage on IBM COS is not supported for IPV6.

Example

Assume you are currently using Centera for system backups, but want to switch to a TSM system. You must turn off the Centera backup option (unless you want to leave that as another option), and turn on the TSM backup option. The commands to do this are highlighted in the example. The show commands are not necessary, but are for illustration only.

```
CLI> show storage-system
```

```
show storage-system
NETWORK :
CENTERA :
TSM :
SCP      : archiving and backing-up
SFTP (formerly FTP)   : archiving and backing-up
AMAZON S3    : archiving and backing-up
IBMcloud   : archiving and backing-up
IBM COS (formerly Cleversafe) : archiving and backing-up
NFS        : backing-up
```

store support state

Enables (**on**) or disables (**off**) the sending of email alerts to the support email address, which can be configured using the **forward support email** command. By default, the support state is enabled (**on**), and the default support email address is support@guardium.com.

Syntax

```
store support state <on | off>
```

Show command

```
show support state
```

store tang server

Sets up the initial connection between the clevis client on a machine to a remote tang server.

You can enter the IP addresses of one or more tang servers. The IP address that is entered first is the primary server, the rest are backup servers. You can change the order of the tang servers by clearing the keys using the CLI command **reset luks keys** and then reentering the tang server addresses by running the **store tang server** command.

Syntax:

```
store tang server
```

Show command:

```
show tang server
```

Shows the most recent tang server to which the Guardium system is connected. The command also displays the backup servers, if any.

store throttle

This CLI command stores the throttle parameters. After entering this command, you must issue the CLI command, restart inspection-core for the changes to take effect.

This command is used to filter out (ignore) large packets. Throttling has two modes: Thresholds, per session - ignore sessions when identifying a long enough burst (duration configurable) of large packets (size configurable) and stop ignoring the session when traffic goes under a certain threshold (also configurable); and, Overall - ignore all packets larger than a certain size (configurable) in all sessions. This throttling mode completely ignores long and excessive non-database packets smaller than a predefined size (useful for VNC clients and other types of white-noise traffic). Use for network traffic through SPAM port or hardware TAP. For S-TAP traffic, only network TCP traffic picked up by PCAP. See also the CLI command, store s2c.

Syntax

```
store throttle [default | size <s> interval <i> trigger <t> release <r>]
```

USAGE: store throttle size S interval I trigger T release R

where 0<=S<=2^17 (bytes), 1<=I,T,R,<=2^31 (seconds)

OR store throttle default

Show command

```
show throttle
```

Throttle parameters:
Packet size: 228000
Time interval: 604800
Trigger level: 10000000
Release level: 10000000

Parameters

- default - Enter the keyword default to restore the system defaults (no other parameters are used). The default throttling parameters are never throttle.
- s - The packet size in bytes, up to a maximum of 217 (131072).
The remaining parameters are in seconds, up to a maximum of 231 (2147483648):
 - i - The time interval
 - t - The trigger level
 - r - The release level

Note: To restore the throttle defaults, use the CLI command, store throttle default.

store timeout

Sets the timeout value of a CLI session and or file server session. The default value is 600 seconds. A timeout will also close the CLI session.

If the file server is stopped because of a timeout, a message will appear, Warning : Fileserver stopped because of timeout. The file upload may not be complete. Stopping the process.

Use the CLI commands, **show timeout db_connection**, to show the socketTimeout value in the conf file, and **store timeout db_connection**, to set the value of the timeout. The value should be greater than 0. The default value is 25000 seconds. These CLI commands are used in managing the communications between the central manager and the managed unit when DNS is not configured.

Syntax

```
store timeout cli_session <n>
store timeout fileserver_session <n>
store timeout db_connection <n>
```

Show command

```
show timeout cli_session 600
show timeout fileserver_session 600
show timeout db_connection 25000
```

store timeout classifier

Sets the number of seconds (0 - 9999) to run classifier queries.

Syntax

```
store timeout classifier <count_query n | sample_query n>
```

Where:

- count_query n - The number of seconds (n) to run a query that determines how many rows are in a particular table.
- sample_query n - The number of seconds (n) to run a query that creates a sample set on which to run the classifier rules. The classifier determines if the table has sensitive data as defined by the rule.

Show syntax

```
show timeout classifier <count_query | sample_query>
```

store transfer-method

Sets the file transfer method. Specify FTP protocol for SFTP.

Syntax

```
store transfer-method <FTP | SCP>
```

Show command

```
show transfer-method
```

Note: Files sent from one IBM Guardium appliance to another (from a collector to an aggregator, for example) are always sent using SCP.

store uid_chain_polling_interval

Set the interval for UID Chain polling with this CLI command. UID chain is a mechanism which allows S-TAP (by way of K-Tap) to track the chain of users that occurred prior to a database connection.

Set the interval to 0 to turn off the UID Chain processing, in order to improve database performance. If the UID Chain processing is turned off, then calculating the UID Chain and updating children sessions are skipped.

Note: When using any database, the UID chain is not logged for all sessions if the session is very short.

Syntax

```
store uid_chain_polling_interval <n>
```

Where n is time in minutes (>= 1 minute; default is 2 minutes). Set N = 0 to turn off the UID Chain processing

Show command

```
show uid_chain_polling_interval
```

store upd_session_end

This CLI command adds an option to skip the update for the session_end time using Session Inference. For more information, see [Session Inference](#).

Syntax

```
store upd_session_end <on | off>
```

Show command

```
show upd_session_end
```

Note: Changes only take effect after the GUI is restarted.

store unit type

Use this CLI command to set unit type attributes for the Guardium appliance. See [Table 2](#) for a description of all unit type attributes you can display with this command.

Syntax

```
store unit type [<manager | standalone | netinsp | stap | mainframe | sink>]
```

Use **store unit type sink** to switch collected DRDA traffic timestamp granularity from 1 millisecond to 1 microsecond.

Show command

```
show unit type
```

The following table describes the Guardium system unit type attributes that you can display with the **show unit type** command. Except where noted, you can set these attributes using the **store unit type** command, and clear them using the **delete unit type** command.

Table 2. Unit type attributes. The unit types that you can see with the **show unit type** command.

| Attribute | Description |
|----------------------|---|
| mainframe | The unit is a mainframe (z/OS®) network inspection appliance. |
| manager | Central manager functions are enabled for this unit. |
| netinsp | Inspection of network traffic is enabled. |
| network route static | Removes one line off the static routing table |

| Attribute | Description |
|------------|---|
| standalone | Local management (independent of a central manager) |
| stap | The unit can receive data from and manage S-TAP and CAS agents. |

Note: You can set the aggregator attribute only when you install Guardium software, and you can only modify it by re-installing the Guardium software.

Unit type attributes

store update_success_value

This CLI command enables or disables the success value flag. When enabled, Guardium updates the SUCCESS field in the GDM_CONSTRUCT_TEXT table for each SQL record.

Syntax

```
store update_success_value [ enable | disable ]
```

Show command

```
show update_success_value
```

store va max_detail

This CLI command helps to regulate the maximum detail records for running query based security assessment tests.

Syntax

```
store va max_detail [on <num> | off]
```

Where

- on<num> enables the record with a value.
- <num> is a number within the range 10 and 2147483647. The default record value is 20000.
- off disables this functionality.

Show command

```
show va max_detail
```

store wkc_configuration

Use this CLI command to integrate and configure IBM Knowledge Catalog with Guardium on managed units. For more information, see [Integrating with IBM Knowledge Catalog for federated data protection](#). If enabled, the CLI requires the IBM Knowledge Catalog URI, user name, and password.

Before you enable the IBM Knowledge Catalog integration with Guardium, you need to store the IBM Knowledge Catalog root certificate on any managed units or stand-alone machines. For more information, see [store_certificate_wkc](#).

Note: The **store wkc_configuration** CLI works only on managed units and stand-alone machines. Use the Guardium to configure the IBM Knowledge Catalog integration on a central manager. For more information, see [Starting the IBM Knowledge Catalog and Guardium Data Protection integration](#).

Syntax

```
store wkc_configuration
```

A list of the available parameters displays,

1. wkc_enabled - false (not enabled)
2. wkc_persistent_cache_enabled - Default = false (disabled).
3. wkc_action_on_unsupported - Default = 1 (deny).

If Guardium receives an unexpected response (or no response) from IBM Knowledge Catalog, you can choose to allow (0) or deny (1) the user access to IBM Knowledge Catalog data assets. The default is 1, that is, treat access to the assets as if the IBM Knowledge Catalog policy rule action **Deny access to data** is triggered. Specify 0 to allow access to data assets, which treats the connection as approved.

4. wkc_cache_ttl - The time-to-live (in minutes) for each decision in the primary cache. Default = 60. Maximum = 1440.
5. wkc_persistent_cache_ttl - The time-to-live (in days) for each decision in the persistent cache. Default = 7. Maximum = 30.
6. wkc_cache_size - Maximum number of cache entries. Default = 1000.
7. wkc_persistent_cache_size - The maximum size of the persistent cache. Default = 100000.
8. wkc_log_level - Default = 4. Log levels range from 1 (FATAL) to 8 (TRACE), with the following meanings,

| Log level | Type | Meaning |
|-----------|-------------|---|
| 1 | FATAL | The application is likely to terminate. |
| 2 | CRITICAL | The application might not continue to run successfully. |
| 3 | ERROR | An operation did not complete successfully, but the application as a whole is not affected. |
| 4 | WARNING | An operation completed with an unexpected result. |
| 5 | NOTICE | An informational message, but with a higher priority. |
| 6 | INFORMATION | An informational message, usually denotes that an operation completed successfully. |
| 7 | DEBUG | A debugging message. |
| 8 | TRACE | A trace message. The lowest priority. |

9. wkc_log_max_files - Default = 10. Maximum = 100.
10. wkc_log_max_file_size - Default = 10 MB. Maximum = 50 MB.
11. wkc_dps_uri - The URI of the IBM Knowledge Catalog service.
12. wkc_asset_user - The owner of this asset. Can be either dbuser or appuser. Default = dbuser
13. wkc_server_auth_username - The IBM Knowledge Catalog user name.

14. wkc_server_auth_password - The password for the associated IBM Knowledge Catalog user.
 15. wkc_column_alias - Specify whether to use an alias for the column name, and if so, what type of alias. Specify one of the following, or click Return to use the default (Column_name).
 - C - Column-name: Default. Use the original COLUMN_NAME as the alias for the full UDF.
 - N - None. Do not use any alias for UDFs.
 - S - Short_udf. Use the short form of the UDF signature.
- For more information, see [Column alias parameter](#) in [Setting up a transformation integration](#).

Store each element of the IBM Knowledge Catalog configuration separately, and then select 0 (zero) to end and Yes to confirm.

To start the IBM Knowledge Catalog integration, you must to set the following parameters:

- 1. wkc_enabled
- 12. wkc_dps_uri
- 14. wkc_server_auth_username
- 15. wkc_server_auth_password

You can use the defaults for the remaining parameters.

Show command

```
show wkc_configuration
```

traceroute

This command is a diagnostic tool that follows the route packets across an IP network.

Syntax

```
traceroute <host> <max hops> <wait time>
```

- host: A valid IP address or hostname
- max hops: The maximum number of hops (default is 30).
- wait time: The timeout to wait for a response to a probe in seconds (default is 5s)

unregister management

The unregister command restores the configuration that was saved when the appliance was registered for central management.

Syntax

```
unregister management
```

Note:

- This command is intended for emergency use only, when the central manager is not available.
- After unregistering using this command, you should also unregister from the central manager (from the Administration Console), since that is the only way the count of managed units will be reduced. The count of managed units is authorized by the product key.

diag CLI command

Use the **diag** CLI command to access troubleshooting and maintenance utilities through the SQLGuard Diagnostics interface.

Use the **diag** command only as directed by Technical Support.

There are no functions that you would perform with this command on a regular basis. Each main menu entry is described in a separate topic.

Troubleshooting and Maintenance Utilities through DIAG:

- Aggregator Fix Schema – brings all imported tables that have older schema than that of the aggregator to the schema of the latest patch level of the aggregator (runs in the background and may take several hours to complete). Note: There may be scenarios in which (a) the aggregator will not have the latest patch level or (b) some of the imported tables are of the latest patch level—resulting in not all imported tables having the latest patch level.
- Aggregator Maintenance – full analysis and recovery of the Aggregator. This utility will collect AGG related logs and place it in the diag export folder, calls the Aggregator Fix Schema to sync the schema of all databases, clean AGG workspace and restart the merge process to ensure full analysis of all imported tables (runs in the background and may take several hours to complete).
- Clean Static Orphans on an Aggregator – This option should be used only by Technical Support and only in those cases where static tables grow too much and needed to be cleaned. This utility cleans all the old construct records that are no longer in use.

Opening the Diagnostics Main Menu

Use the **diag** command to open the SQLGuard Diagnostics menu as follows:

1. At the command line prompt, log into the Guardium® appliance with CLI.

Note: To use the CLI, the Guardium user must have a CLI or admin role, or CLI does not start. Use the **accessmgr** to assign CLI and admin roles.

Note: To use the **diag** command, the Guardium user must have an assigned CLI or admin role. The only user who has a CLI role by default is admin. A user with a CLI or admin role can enter the **diag** command, use the **unlock admin** and **unlock accessmgr** CLI commands, and use the **export audit-data** CLI command without restrictions. A user with the CLI role does not have to enter user name and password required of a GUI login and does not go through any further role check.

In addition, as a Guardium user, you must have an assigned diag role on the Guardium system to use the **diag** command. By default, only admin has this assigned role. Access to diag is allowed based on the role assignment of this user (access to diag is permitted only if this user has the diag role). The **accessmgr** assigns diag roles.

2. After starting CLI, enter the **diag** command (with no arguments) at the command line prompt to open the SQLGuard Diagnostics window.
3. Do one of the following to move the option selection cursor:
 - Type the desired entry number (the selection cursor moves to the selected entry).
 - Use the Up or Down arrow key to select an entry.
4. Click the Spacebar, the Left arrow key, or the Right arrow key to move the command selection cursor in the display.
5. Perform an action by selecting the appropriate option in the display area and then doing one of the following:
 - Select the appropriate command with the command selection cursor, then click Enter.
 - Click on the appropriate action command.

About the diag Output

The diag command creates output in two directories:

- .../guard/diag/current
- .../guard/diag/depot

You can access the output through the **fileserver** CLI command. For more information, see [fileserver](#).

Each directory is described in the following subsections.

.../guard/diag/current Directory

Most output from the diag commands is written in text format to the current directory. For most commands, this directory contains a separate output file. Each time you run the same command, output is appended to the single file for that command. For a smaller number of commands, a separate file is created for each execution, usually incorporating a date and time stamp in the filename.

We recommend that you “clean up” after each session, so that you are not looking at old information in subsequent sessions. When you pack files to a single compressed file for export, all of the files in the current directory are deleted. Alternatively, use the Delete recordings option from the Output Management menu to delete individual files.

The files in the current directory are easy to identify since the names are created from menu and command names. For example, after you use the File Summary command from the System Interactive Queries menu, a file named interactive_filesummary.txt is created in the current directory.

If you look at the current directory while in the process of using a command, you may see a hidden temporary file with the same name as the one that will contain the output for that command. The temporary file will be removed when the output is appended to the command output file.

.../guard/diag/depot Directory

When you pack the diag output files in the current directory to a compressed file (to send to Guardium Technical Support, for example), it is stored in the depot directory. The filename is in the format diag_session_<dd_mm_hhmm>.tgz, where the variable portion of the name indicates when the file was created. For example, a file created at 12:15 PM on May 20th would be named as follows: diag_session_20_5_1215.tgz.

After exporting files (see the Export recorded files topic), you can remove them from the depot directory using the Delete recordings command of the Output Management menu.

1 Output Management

The Output Management commands control what is done with the output produced by the diag command. Each Output Management command is described separately.

1.1 End and pack current session

Use this command to pack all diagnostic files in the current directory into a single compressed file, and remove those files from the current directory. When you enter this command, there is no feedback to indicate that the command has completed. You can verify that the command has finished by displaying the directory of the depot directory. When the command completes, there is a file named in the following format: diag_session_<mm_dd_hhmm>.tgz, where the variable portion of the name is a date and time stamp, as described previously. Use the Export recorded files command of the Output Management menu to send the file to another system.

1.2 Delete recordings

Use this command to delete files in the depot or current directory. (To delete only the current session files, use the Delete current session files command.) When you enter this command, the depot directory structure displays:

You can navigate the directories using the Up and Down arrow keys and clicking Enter. For example, selecting .. and clicking Enter moves the selection up one level in the directory structure.

You could then select the current directory and click Enter, to navigate down to that folder and delete individual command output files. Note that you can navigate to other directories, but you cannot delete files except from the current and depot directories.

When you have selected the file you want to delete, click Enter.

Caution: You will not be prompted to confirm the delete action

1.3 Export recorded files

Use this command to send a file from the depot directory to another site. To export a file:

1. Select Export recorded files from the Output Management menu. The depot directory displays.
2. Select the file to be sent or use the .. and ./ entries to navigate up or down in the directory structure. (However, keep in mind that you can only export files from the depot directory.)

3. With the file to be transmitted selected, click Enter.
4. You are prompted to select FTP or exit. Select FTP and click Enter.
5. You are prompted to supply a host name. Enter the host name of the receiving system (or its IP address), and click Enter.
6. You are prompted for a user name. Enter a user account name for the receiving system, and click Enter.
7. You are prompted for a password. Enter the password for the user on the receiving system.
8. You are prompted to identify a directory to receive the sent file on the receiving system. Enter the path relative to the ftp root of the directory to contain the file on the receiving system and click Enter.
9. You are prompted to confirm the details of the transfer (the file to be sent and its destination). Click Enter to perform the transfer, or select Cancel and click Enter to start over.
10. You are informed of the success (or failure) of the operation.

1.4 Delete current session files

Use this command to delete files created during the current session.

1.5 Exit

Use the Exit command to return to the main menu.

2 System Static Reports

Use the System Static Reports command of the Main Menu to produce an extensive set of reports.

1. Select System Static Reports from the Main Menu. You are informed that the process is running.
 2. After the report has been created, it displays in the viewing area. Note that this report is lengthy and may be easier to view using a text editor, after exporting it to a desktop computer).
- Use the Up and Down arrow keys to scroll up or down in the report. When you are done viewing the report, click Enter to return to the Main Menu.

System Static Reports Overview

The following subtopics provide an outline of the major components of the System Static Reports output. The fragments of output shown are intended to illustrate the type and level of information contained in the report, rather than provide a detailed description of the actual contents (that is beyond the scope of this document).

System Configuration Information

The System Static Reports output describes the build version, the patches applied, the current system up time, and name server information:

```
Build version: 34e1eb12eb68ba76cb49028251c9a0d6 /opt/IBM/guardium/etc/cvstag
Patches:
2009/02/22 16:16:50: START Installation of 'Update 5.0'
2009/02/22 16:18:04: Installation Done - Successfully Installed

< lines deleted... >

Current uptime:
09:03:43 up 6 days, 17:34, 1 user, load average: 0.44, 0.50, 0.41
System nameservers:
192.168.3.20
DB nameservers:
192.168.3.20
Gateway: 192.168.3.1 (system) 192.168.3.1 (def)
```

Next, the file system information displays (shown partially):

```
Filesystem      Size  Used Avail Use% Mounted on
/dev/hdc3       2.0G  1.1G  813M  58% /
/dev/hdc1        97M   9.2M  83M   10% /boot
none            504M    0   504M   0% /dev/shm
/dev/hdc2       71G   1.2G  66G   2% /var
              total: used: free: shared: buffers: cached:
Mem: 1055199232 1041711104 13488128          0 63275008 186220544
Swap: 536698880 295432192 241266688
MemTotal: 1030468 kB
MemFree: 13172 kB

< lines deleted... >
```

This is followed by information about the mail and SNMP servers configured:

```
SMTP server: 192.168.1.7 on port 25 : REACHABLE
SMTP user: undef
SMTP password: undef
SMTP auth: NONE
SNMP trapsink: undef UNREACHABLE
SNMP trap community: undef
SNMP read community: undef
```

The final section of the system configuration section describes the network configuration for the unit: IP address, host and domain names, etc:

```
ens32:          192.168.3.101 (system) 192.168.3.101 (def)
hostname:           (system) g1 (def)
domain:            (system) guardium.com (def)
mac address: 00:04:23:A7:77:F2 (MAC1) 00:04:23:A7:77:F2 (MAC2)
unit type: 548 Standalone STAP
```

Internal Database Information

The next major section of the System Static Reports output contains information about the internal database status and threads (only the first few threads are shown):

```
uptime 77097 seconds.
27 threads.
78545028 queries.

+-----+-----+-----+-----+
| Id | User      | Host          | db    | Command | Time   | State  |
+-----+-----+-----+-----+
1137	enchantedg	localhost	TURBINE	Sleep	26
1257	enchantedg	localhost.localdomain:33587	TURBINE	Sleep	0
1258	enchantedg	localhost.localdomain:60409	TURBINE	Sleep	7716
1259	enchantedg	localhost.localdomain:48233	TURBINE	Sleep	322

< lines deleted... >
```

The list of threads is followed by an analysis of table status.

Web Servlet Container Information

The next several sections of the System Static Reports output contain information about the Web servlet container environment (Tomcat):

```
=====
Currently defined Tomcat port is 8443.
The TOMCAT daemon is running and listening on port(s): 8005 8443.
Currently OPEN ports
java run by tomcat on port *:8443

< lines deleted... >
=====
```

```
These are the nanny latest actions:
May 19 14:13:09 guard nanny:[5528]: Also checking tomcat.
May 19 14:13:09 guard nanny:[5528]: Going for my initial nap.

< lines deleted... >
```

```
This is the TOMCAT command line:
 463 sh -c ps -o pid,cmd -e | grep Dcatalina.base
21917 grep Dcatalina.base.
```

Inspection Engine Information

The next major section of the System Static Reports output contains information about the inspection engine:

```
=====
This is the SNIF (pid: 13036) command line: 13036 /opt/IBM/guardium/bin/snif.
This is the SNIF status:
Name:           snif
State:          R (running)
Tgid: 13036

< lines deleted... >
=====
```

```
Current timestamp is 2009-05-20 11:56:41
This is the last timestamp at GDM_CONSTRUCT_INSTANCE: 2009-05-20 11:56:41
This is the last timestamp at GDM_EXCEPTION: 2009-05-20 11:56:41
This is the last timestamp at GDM_POLICY_VIOLATIONS_LOG: 2009-05-20 11:56:41

=====
```

```
Snif buf usage at Fri May 20 11:56:44 2009:
100 204800 buffers out of 204800
126 connection used, 32642 unused, 0 dropped (sniffer), 9 ignored (analyzer)
0 bytes lost, 60 connections ended, 601752099 bytes sent, 579063 request sent
Dropped Packets: 0 buffer full, 0 too short , 451 ignored
time now is 1116604603
Analyzer/Parser buffers size: 6 (66533) 0 (62902)
ms-tsql-logger 0 (11331)
syb-tsql-logger 0 (70)
ora-tsql-logger 79 (67803)
db2-sql-logger 0 (20544)

< lines deleted... >
```

IP Tables Information

The next major section contains information about the IP tables:

```
=====
IPTABLES:
-----
      tcp  --  192.168.2.0/24      192.168.1.0/24      tcp  spts:1521:60000  set 0x23
      tcp  --  192.168.1.0/24      192.168.2.0/24      tcp  dpts:1521:60000  set 0x22
< lines deleted... >
```

S-TAP Information

The next major section contains S-TAP® information:

```
=====
STAP:
-----
  0      0 ACCEPT    tcp  --  *      *  0.0.0.0/0      0.0.0.0/0      tcp spt:9500
  0      0 ACCEPT    tcp  --  *      *  0.0.0.0/0      0.0.0.0/0      tcp dpt:9500
2696  148K ACCEPT   tcp  --  *      *  0.0.0.0/0      0.0.0.0/0      tcp spt:16016
2835  175K ACCEPT   tcp  --  *      *  0.0.0.0/0      0.0.0.0/0      tcp dpt:16016

< lines deleted... >
```

IP Traffic Information

The next major section contains IP traffic information:

```
IP traffic statistics.
OUTPUT OF ens32
Fri May 20 11:57:04 2012; ***** Detailed interface statistics started *****
*** Detailed statistics for interface ens32, generated Fri May 20 11:58:04 2009

< lines deleted... >

OUTPUT OF ens192
Fri May 20 11:57:04 2012; ***** Detailed interface statistics started *****
*** Detailed statistics for interface ens192, generated Fri May 20 11:58:04 2009

Total:          82440 packets, 53892382 bytes
           (incoming: 82440 packets, 53892382 bytes; outgoing: 0 packets, 0 bytes)
IP:            82440 packets, 52632747 bytes
           (incoming: 82440 packets, 52632747 bytes; outgoing: 0 packets, 0 bytes)

< lines deleted... >
```

Information Engine STDERR and STDOUT Information

The next section contains the last messages output by the sniffer:

```
Snif  STDERR:
< lines deleted... >

Snif STDOUT:
Fri_20-May-2009_04:04:35 : Guardium Engine Monitor starting
Fri_20-May-2009_04:14:37 : Guardium Engine Monitor starting
Fri_20-May-2009_04:24:38 : Guardium Engine Monitor starting

< lines deleted... >
```

Import Directory Information

The next section lists the import directory contents:

```
These are the contents of the importdir directory:
total 0
```

Aggregator Activity Information

This section lists aggregator activities (there are none in the example):

```
=====
This is the aggregator last activities:
```

Audit Report

This section lists the following summary information (see example):

```
=====
Range of time in logs: 01/14/10 13:12:26.348 - 01/18/10 12:48:01.073
Selected time for report: 01/14/10 13:12:26 - 01/18/10 12:48:01.073
Number of changes in configuration: 4 - changes to the audit configuration
Number of changes to accounts, groups, or roles: 0
Number of logins: 22 - logins into the machine - ssh and console
Number of failed logins: 114
Number of authentications: 22 - "su", etc.
Number of failed authentications: 5
Number of users: 2
Number of terminals: 18
Number of host names: 9
Number of executables: 7
Number of files: 0
Number of AVC's: 0
Number of MAC events: 0
Number of failed syscalls: 0
Number of anomaly events: 3
Number of responses to anomaly events: 0
```

```
Number of crypto events: 0
Number of keys: 0
Number of process IDs: 9173
Number of events: 98669
=====
```

Anomaly Report

This section lists the following (see example):

```
=====
# Date Time Type Exe Term Host AUID Event
=====
1. 01/14/10 13:16:02 ANOM_PROMISCUOUS /usr/sbin/brctl (none) ? -1 8 - this is expected
to appear - it means the bridge is listening to all traffic
```

Authentication Report

This section lists the following (see example):

```
=====
# Date Time Type Exe Term Host AUID Event
=====
1. 01/14/10 13:13:22 tomcat ? console /bin/su yes 4
2. 01/14/10 13:16:44 tomcat ? console /bin/su yes 11
3. 01/14/10 13:16:44 tomcat ? console /bin/su yes 17
4. 01/14/10 13:16:45 tomcat ? console /bin/su yes 23
5. 01/14/10 13:16:48 tomcat ? console /bin/su yes 29
6. 01/14/10 13:22:29 tomcat ? ? /bin/su yes 155
7. 01/14/10 13:28:10 ? ? ttys /bin/login no 252
8. 01/14/10 13:28:20 ? ? ttys /bin/login no 254
```

Login Report

This section lists the following (see example):

```
=====
# Date Time Type Exe Term Host AUID Event
=====
1. 01/14/10 13:22:15 root 192.168.2.9 sshd /usr/sbin/sshd no 142
2. 01/14/10 13:22:15 root 192.168.2.9 sshd /usr/sbin/sshd no 143
3. 01/14/10 13:22:17 root 192.168.2.9 sshd /usr/sbin/sshd no 144
4. 01/14/10 13:22:17 root 192.168.2.9 sshd /usr/sbin/sshd no 145
5. 01/14/10 13:22:20 root 192.168.2.9 sshd /usr/sbin/sshd no 146
```

3 Interactive Queries

Select System Interactive Queries from the main menu to open the Interactive Queries menu. (Use the Down arrow key to scroll past the tenth item to see all items on this menu.)

In addition to displaying the requested information, each interactive query command creates output in a separate text file in the current directory. See the Overview topic for more information about the files created.

Each command is described in the following sections.

3.1 Files Changed

Use the Files Changed command to display a list of files changed either before or after a specified number of days.

1. Select Files Changed from the Interactive Queries menu. You are prompted to enter a number days. Type a number and click Enter.
2. You are asked if you are interested in the files changed before or after that number of days. Select 1 or 2 and click Enter.
3. The full directory path for each changed file is displayed. Note that if not all data fits in the display area, use the Up and Down arrow keys to scroll through the data. The current position in the file is indicated by the number in the display. The white bars in the display area indicate the presence of more data with a plus sign.

3.2 List Folder

Use this command to list the contents of various directories.

1. Select List Folder from the Interactive Queries menu.
2. You are prompted to select a directory. Select a directory and click Enter. The selected directory is displayed. Remember that if multiple commands of the same type are issued, the data for each execution of the command is appended to the single text file maintained for that command.
3. Click Enter or click Exit when you are done.

3.3 Summarize Folder

Use the Summarize Folder command to display the output of the du (Disk Usage) command:

1. Select Summarize Folder from the Interactive Queries menu. There are no prompts. You are presented with a display of disk use for various directories.
2. Use the Up and Down arrow keys to scroll through the directories.
3. Click Enter or click Exit when you are done.

3.4 File Summary and Export

Use this command to list all or some portion of a log file.

1. Select File Summary from the Interactive Queries menu.
 2. You are prompted to select a file. Use the Up and Down arrow keys to scroll the selection cursor to the file you want to view.
 3. Click Enter or click OK.
 4. You are prompted to select the number of lines to display. Make your selection and click Enter.
 5. You are prompted to enter an optional search string. Use this box if you are searching for a particular log message (you can enter a regular expression). Otherwise leave the box empty and click Enter.
 6. Following the prompt, click Enter to answer yes, meaning that only unique messages will be displayed. Otherwise select No and click Enter (all messages will be displayed).
- Be aware that when the Summary Style is used, variables are replaced by the pound sign character (#). For some log data containing variables such as IP addresses or dates, the replacements can be extensive.

3.5 Test Email

Use this command to send a test email using the configured SMTP server.

1. Select Test Email from the Interactive Queries menu.
2. You are prompted to select a recipient. Select Custom and click Enter.
3. You are prompted to supply an email address. Type an email address and click Enter. You will be informed of the output of the operation. Note that on the Administration Console, the Test Connection link in the SMTP pane of the Alerter configuration panel only tests that an SMTP port is configured, not that mail can actually be delivered via that server. You can use this command to test email delivery without having to configure and trigger a statistical or real-time alert, or an audit process notification.

3.6 Test SNMP

Use this command to send a test SNMP trap to the configured SNMP server.

1. Select Test SNMP from the Interactive Queries menu.
2. You are informed of the activity and the results. Note that on the Alerter Configuration panel, the Test Connection link in the SNMP pane only tests that an SNMP port is configured, not that a trap can actually be delivered via that server. You can use this command to test trap delivery without having to configure (and trigger) a statistical or real-time alert, or an audit process notification.

3.7 Report Query Data

Use this command to display the actual select statement used for a report query. This might be useful if a user-written report is producing unexpected output.

1. Select Report Query Data from the Interactive Queries menu.
2. You are prompted to make a selection from a list of report titles. Use the Up and Down arrow keys to select an entry and click the Enter key. Each entry in this list is a Report entity. All pre-defined reports are listed first. These are numbered in the range 100-225 (for version 3.6.1 – the numbers will most likely grow incrementally with each release, as more pre-defined reports are created). User written reports are listed following the pre-defined reports, beginning with number 20001 (for version 3.6.1).

The selected report select statement will be displayed.

3.8 GDM Queries

Use this command to display a count of observed SQL calls during a 100 second interval.

1. Select GDM Queries from the Interactive Queries menu.
2. A message displays requesting your patience. Select yes to continue. The CMD_CT column on the display lists the number of observed SQL calls from the specified clients to the specified servers.
3. Click Enter when you are done viewing the report.

3.9 Generate TCP Dump

Use this command to create a TCP dump. For this command, output is written to a command file only and not to the screen. Unlike most other commands, a separate file is created in the current directory for each execution of this command. The file name is in the format: tcpdump_<mmyyyy-hhmmss>, where the variable portion is a date and time stamp: mmyyyy is the month and year, and hhmmss is the hours, minutes, and seconds.

1. Select Generate TCP dump from the Interactive Queries menu.
2. You are prompted to select an interface. Select a port and click Enter.
3. You are prompted for an optional filter IP address. If you are interested in traffic from only a specific address, enter that IP address and click Enter. Otherwise, just click Enter.
4. You are prompted for an optional port number. If you are interested in traffic from only a specific port, enter that port number and click Enter. Otherwise, just click Enter.
5. You are prompted to select how many seconds of traffic to capture. Select a number of seconds and click Enter.
6. You are prompted to click Enter to start collecting data. Click Enter. You are returned to the menu after (approximately) the specified number of seconds.
7. To view the TCP dump data, select the Read TCP dumps command or export the file (see Export Reported Files on the Output Management menu, described previously).

3.10 Read TCP Dumps

Use this command to display a TCP dump file created previously.

1. Select Read TCP dumps from the Interactive Queries menu.
2. You are prompted to select file. The TCP dump files are listed from oldest to newest. The file name is in the format: `tcpdump_<mmddyy-hhmmss>`, where the variable portion is a date and time stamp: mmddyy is the month, day, and year; and hhmmss is the hours, minutes, and seconds. Select the file you want to view and click Enter.
3. The selected file displays. Use the Up and Down arrow keys to scroll through the display and click Enter when you are done.

3.11 Watch Buffer

Use this command to watch activity in the Guardium buffers:

1. Select Watch Buffer from the Interactive Queries menu. The display is updated every second.
2. Click Ctrl-C to close the display.

3.12 SLON Utility

Use this command to run the slon utility, which tracks packets. Typically, you would only run this command as directed by Technical Support. For this command, output is not written to the screen. Output is written to one of two command files in the current directory, for each execution of the command: `apks.txt.<day_dd-mmm-yyyy_hh.mm.ss.ttt>` OR `requests.txt.<day_dd-mmm-yyyy_hh.mm.ss.ttt>`

The variable portions or the file names are date and time stamps. For example, `apks.txt.Fri_20-May-2011_08.52.00.789`.

1. Select Slon Utility from the Interactive Queries menu.
2. Select the action to be performed and click OK. The choices are:
 - (a) to dump Analyzer rules info
 - (f) to filter Analyzer packets based on IP and/or mask
 - (p) to dump packets to apks.txt
 - (l) to dump logger requests to requests.txt
 - (m) to dump STAP packets (Select how long to run. Wait for completion and then check the msg-dump file under `/var/log/guard/diag/current/tap/`)
 - (r) to record IPQ traffic
 - (s) to dump State machine info
 - (t) to configure throttle parameters
3. Regardless of your selection, you will be prompted to select the time period for the activity. Select a time period and click Enter.
4. You are notified that the program will run for the specified time and prompted to click Enter. Click Enter and wait.
5. When processing completes, a message will be displayed. You can use the File Summary command to display the output of this command. Because this command can produce a large amount of data, you will probably want to export the file to another system, where you can view the contents using a text editor. (Pack the current session data, and export the recordings as described earlier in this section.)

3.13 Show Indexes

Use this command to show indexes for various internal tables:

1. Select Show Indexes from the Interactive Queries menu.
2. You are prompted to select a table. Select a table and click Enter to display the indexes for that table.
3. Use the Up and Down arrow keys to scroll through the display. Click Enter when you are done.

3.14 S-TAP Check

Use this command to display S-TAP definitions and traffic information:

1. Select S-TAP Check from the Interactive Queries menu.
2. The system's unit type displays in numeric format. Click Enter.
3. You are prompted to select the number of seconds to monitor the S-TAP traffic. Use the Up and Down arrow keys to make a selection and click Enter.
4. You are informed of approximately how long to wait for output, and prompted to click Enter. Click Enter.
5. The S-TAP Definitions and Server Traffic reports display. Click Enter when you are done viewing the report.

3.15 Interface Link Status

Use this command to display interface link status.

1. Select Interface link status from the Interactive Queries menu.
2. The status of all interfaces displays. Use the Up and Down arrows to scroll through the display.
3. Click Enter when you are done. Note that this command displays the link status only. To display interface configuration information, use the **show network interface all** CLI command.

3.16 Show Throttle Data

Use this command to display throttle data.

1. Select Show Throttle data from the Interactive Queries menu.
2. Click Enter and wait 3 seconds for throttle statistics.
3. Use the Up and Down arrows to scroll through the display, and click Exit when you are done.

3.17 Generate TCP dump and slon

Use this command to create a TCP dump and run the slon utility, which tracks packets. Only run this command as directed by Technical Support. For more information, see [Generate TCP dump](#) and [Slon utility](#).

3.18 Generate SSL dump

Use this command to create a SSL dump..

1. Select Generate SSL dump from the Interactive Queries menu.
2. Select an interface and click OK. Enter filter IP address and click OK. Enter filter port number and click OK.
3. Select how long to run and click OK. Click OK and wait the specified time in order to gather TCP dumps.
4. If you wish to view SSL dumps, click OK.
5. Click Exit when you are done.

3.19 View bash history

Use this command to display bash history.

1. Select View Bash History from the Interactive Queries menu.
2. Click OK.
3. Use the Up and Down arrows to scroll through the display, and click Exit when you are done.

3.20 Generate GDM_Error dump

Use this command to create GDM_ERROR dumps..

1. Select Show Generate GDM_ERROR dump from the Interactive Queries menu.
2. Click OK and then enter password. Click Enter.
3. Use the Up and Down arrows to scroll through the display, and click Exit when you are done.

3.21 Prepare Tomcat Memory dump

When Tomcat has a first outOfMemory error, it will do a memory dump to /var/tmp/tomcat/tomcat.dmp. Use this command to compress, encrypt and move this file to /var/log/guard/diag/tomcat/ for fileserv to retrieve.

1. Select Prepare Tomcat Memory dump from the Interactive Queries menu.
2. Click OK.
3. Use the Up and Down arrows to scroll through the display, and click Exit when you are done.

3.22 Extended Network Information

Click on Extended Network Information option under System interactive query to display the network diagnostics information.

Example

SQLGuard Diagnostics

Network Parameters from ADMINCONSOLE_PARAMETER:

SYSTEM_NETMASK1: 255.255.255.0

SYSTEM_DOMAIN:

SYSTEM_DEFAULT_ROUTE:

SYSTEM_DNS1:

SYSTEM_DNS2:

SYSTEM_DNS3:

TOMCAT_IP:

MANAGER_IP:

HOST_MAC_ADDRESS:

SECOND_DEVICE:

3.23 Generate TCP dump in rotation

This selection is different from other diag selections in the section called Generate TCP and Generate TCP and slon.

For Generate TCP dump in rotation, enter Filter IP address (enter blank for all IPs). Enter Filter Port number. For the question, How long to run? if the TCP dump in rotation is already running, choose the option “Rotation OFF” or “Rotation” (ON). If Rotation is selected, add file size.

The TCP dump will be output to /var/log/guard/tcp.bin1 and /var/log/guard/bin2 in rotation.

Select TCP dump in rotation again to stop the process loop_tcpdump.sh.

4 Perform Maintenance Actions

Select the Perform Maintenance Actions option from the Main Menu to open the Maintenance menu. Use these commands only under the direction of Technical Support. These do not need to be run on a regular basis.

4.1 TURBINE analyze (update index cardinality)

Use this command to optimize index cardinality on Guardium's internal database. A progress bar displays while the operation is running. When the operation completes, you are returned to the Maintenance menu.

4.2 TURBINE optimize (rebuild indexes, takes longer)

Use this command to analyze and re-index Guardium's internal database.

1. Select TURBINE optimize (index cardinality) from the Maintenance menu. A progress bar displays while the operation is running. When the operation completes, you are returned to the Maintenance menu.

4.3 Clean disk space

Use this command to clean unused disk space. You are returned to the Maintenance menu when the procedure completes.

1. Select Clean disk space from the Maintenance menu. You will be prompted to select a directory.
2. Select the directory from which you want to remove files. The contents of the directory will be listed, and you will be prompted to confirm that you want to remove all files.
3. When the operation completes, you are returned to the Maintenance menu.

4.4 RAID maintenance

Use this command only under the direction of Technical Support. This command provides access to the Management Menu of the RAID controller utility program, which can be used to display the status of the RAID drives. If your system does not have a RAID controller, an error message displays if you select this command. You must be extremely careful when using the RAID controller utility program, since several of the functions provided will erase all information on the disk.

4.5 Application Debugging Utility

Use this command to turn debugging on or off. You are prompted to enable or disable logging, or to reset the system defaults.

4.6 Modify TURBINE watchdog time threshold

Use this option to change the timeout limit for long queries.

4.7 Force unrecoverable MySQL to start

Use this option only when directed to do so by Technical Support.

4.8 Transfer Backups & System Recovery

Use this command to restore a backed up version of the internal database. You will be prompted to confirm the operation.

4.9 Tomcat logging level

Use this command to select the component debug level. Choose one of the following options:

Classifier, Data Level Security, Workflow, or Other.

Choose Classifier to select debug level options: ERROR, WARN, INFO, DEBUG, ALL.

Choose DLS (data level security), Workflow, or Other (text input) to select debug level options: ERROR, WARN, INFO, DEBUG, ALL.

If Other is chosen (text input separated by ';'), enter valid components (dls, workflow, audit, customtable, gui, other, job).

4.10 Aggregator Maintenance

Full analysis and recovery of the Aggregator. This utility will collect AGG related logs and place it in the diag export folder, calls the Aggregator Fix Schema to sync the schema of all databases, clean AGG workspace, and restart the merge process to ensure full analysis of all imported tables (runs in the background and may take several hours to complete).

4.11 Aggregator Fix Schema

Brings all imported tables to the schema of the latest patch level (runs in the background and may take several hours to complete).

4.12 Clean Static Orphans

This option should be used only by Technical Support and only in those cases where static tables grow too much and needed to be cleaned. This utility cleans all the old construct records that don't have any Instances associated with them. A progress message will display during the Clean Static Orphans (for use on collector or aggregator).

5 Exit to CLI

Select Exit to CLI on the Main Menu. Click Enter to close the diag command and return to the command line interface.

File handling CLI Commands

Use these commands to backup and restore system information. Many of these tasks can be performed from Guardium® user interface.

About Archived Data File Names

When Guardium data is archived (or exported to an aggregator), there is a separate file for each day of data. Depending on how your export/purge or archive/purge operation is configured, you may have multiple copies of data exported for the same day. Archive and export data file names have the same format:

<daysequence>-<hostname.domain>-w<run_datestamp>-d<data_date>.dbdump.enc

- daysequence is a number representing the date of the archived data, expressed as the number of days since year 0. The same date appears in yyyy-mm-dd format in the data_date portion of the name.
- hostname.domain is the host name of the Guardium appliance on which the archive was created, followed by a dot character and the domain name.
- run_datestamp is the date that the data was archived or exported, in yyymmdd.hhmmss format.
- data_date is the date of the archived data, in yyyy-mm-dd format.

For example: 732423-g1.guardium.com-w20050425.040042-d2005-04-22.dbdump.enc

backup config

These commands back up and restore configuration information from the internal administration tables. The backup config command stores data in the /media/backup directory. The backup config command removes license and other machine-specific information. The backup system command provides a more comprehensive backup of the configuration and the entire system.

Syntax

backup config

restore config

backup system

This topic applies to backup and restore operations for the Guardium internal database. You can back up or restore data, configuration information, or both. These commands stop all inspection engines and web services and restart them after the operation completes.

Use the **restore backup** command to restore a backup to the latest version of Guardium.

Note: The restore backup command can only restore files from Guardium V10.1.3 or later. For more information, see [restore backup](#).

For all backup, import, and restore commands, you receive a series of prompts to supply some combination of the following items, depending on which storage systems are configured, and the type of restore operation. Respond to each prompt as appropriate for your operation. [Table 1](#) describes the information for which you might be prompted.

Note:

- One copy of the SCP/SFTP/TSM/Centera file transfer is saved, whether or not the transfer is successful. Certain files can take hours to regenerate (such as system backup), so having an available copy (in particular if the file transfer failed) can be a valuable time-saver. Only one copy of each type of file is retained (that is, one archive, one system backup, one configuration backup, and so on).
- The **backup system** command copies the current license, metering and number of data sources, and then backs up the data. Use **restore backup** to restore the data and then restore the license, metering, and number of data sources.
- When configuring backups, a value of zero '0' for the port number indicates that the default port is being used for that protocol.

Table 1. backup system parameters

| Item | Description |
|--|--|
| • AmazonS3
• Centera
• IBM Cloud
• IBM COS
• NFS
• SCP
• SFTP
• TSM | Select the method to use to transfer the file. Storage methods display only if they are enabled. For more information, see the store storage-system command. |
| Data or Configuration | Select Configuration to back up definitions and configuration information only, or select Data to back up data in addition to configuration information. |
| restore from archive or restore from backup | Select restore from archive to restore archived data, or select restore from backup to restore configuration information. |

| Item | Description |
|-------------------|---|
| normal or upgrade | If restoring from the same software version of Guardium, select normal. If restoring configuration information following software upgrade of the Guardium appliance, select upgrade. |
| host | The remote host for the backup file. |
| remote directory | The directory for the backup file. For SFTP, the directory is relative to the SFTP root directory for the SFTP user account used. For SSH, the directory path is a full directory path. For Windows SSH servers, use Unix-style path names with forward slashes, rather than Windows-style backslashes. |
| username | The user account name to use for the operation (for backup operations, this user must have write/execute permission for the directory specified). Note: For Windows, a domain user is accepted with the format of domain\user |
| password | The password for the username. |
| file name | The file name for the archive or backup file.
You can select multiple files by using the wildcard character (*) in the file name when using FTP, SCP, and Snapshot transfer methods. The wildcard character is not supported with TSM or Centera. |
| Centera server | The Centera server name. If using PEA files, use the following format: <Host name/IP>?<full PEA file name>, for example: 128.221.200.56?var/centera/us_profile_rwqe.pea.txt |
| Centera clipID | For a Centera restore operation, the Content Address returned from the backup operation. For example: 6M4B15U4JM4LBeDGKCPF9VQO3UA |

After you supply all of the information required for the backup or restore operation, a series of messages displays informing you of the results of the operation. For example, at the end of a successful restore backup operation, a message similar to the following is sent to the

/var/IBM/Guardium/log/diag/depot/upgrade_<TimeStamp>.log file:

```
2019-05-16-165208 Upgrade of v10.0 to v11.0.0 completed successfully
```

Prevent backup or archive scripts from filling up /var

The backup process will check for room in /var before running and fail. This process will also warn the user if there is insufficient space for backup.

The archive process will check the size of the static tables and make sure there is room in /var to create the archive.

An error is now logged in the logfile and GUI if the backup is over 50%

Example:

```
ERROR: /var backup space is at 60% used. Insufficient disk space for backup. CLI> backup system 1. DATA 2.
CONFIGURATION Please enter the number of your choice: (q to quit) 1 1. SCP 2. CONFIGURED DESTINATION Enter the
number of your choice: (q to quit) 2 Make sure destination is configured in the GUI under the System Backup option Please wait,
this may take some time.
```

delete audit-data

Use this command only under the direction of Guardium Support. This command is used to remove compressed audit data files. You will be prompted to enter an index number to identify the file to be removed. See Archived Data File Names, for information about how archived data file names are formed.

You will be prompted to identify the file to be removed.

Syntax

```
delete audit-data
```

export audit-data

Exports audit data from the specified date (yyyy-mm-dd) from various internal Guardium tables to a compressed archive file. The data from a specified date will be stored in a compressed archive file, in the /var/dump directory. The file created will be identified in the messages produced by the system. See the example. Use this command only under the direction of Guardium Support.

Note: Only users with admin role may run this command .

Syntax

```
export audit-data <yyyy-mm-dd>
```

Example

```
export audit-data 2005-09-16 2005-09-16
```

Generates a set of messages similar to the following:

```
Extracting GDM_ACCESS Data ...
Extracting GDM_CONSTRUCT Data ...
Extracting GDM_SENTENCE Data ...
Extracting GDM_OBJECT Data ...
Extracting GDM_FIELD Data ...
Extracting GDM_CONSTRUCT_TEXT Data ...
Extracting GDM_SESSION Data ...
Extracting GDM_EXCEPTION Data ...
Extracting GDM_POLICY_VIOLATIONS_LOG Data ...
Extracting GDM_CONSTRUCT_INSTANCE Data ...
Generating tar file ... /var/csvGenerationTmp ~
GDM_ACCESS.txt
GDM_CONSTRUCT.txt
GDM_CONSTRUCT_INSTANCE.txt
GDM_CONSTRUCT_TEXT.txt
GDM_EXCEPTION.txt GDM_FIELD.txt
GDM_OBJECT.txt
GDM_POLICY_VIOLATIONS_LOG.txt
```

```
GDM_SENTENCE.txt
GDM_SESSION.txt ~
Generation completed, CSV Files saved to /var/dump/732570-supp2.guardium.com-w20050919110317-d2005-09-16.exp.tgz ok
```

The data from each of the named internal database tables is written to a text file, in CSV format. The name of the archive file ends with exp.tgz and the remainder of the name is formed as described in About Archived Data File Names.

You can use the export file command to transfer this file to another system.

export file

This command exports a single file named filename from the /var/IBM/Guardium/data/dump, /var/log or /var/IBM/Guardium/data/importdir directory.

Use this command only under the direction of Guardium Support. To export Guardium data to an aggregator or to archive data, use the appropriate menu commands on the Administration Console panel.

Syntax

```
export file </local_path/filename> <user@host:/path/filename>
local_path must be one of the following: /var/IBM/Guardium/data/dump, /var/log or /var/IBM/Guardium/data/importdir
```

export-public-transfer-key

This command starts a script that forces a new set of ssh keys onto the specified remote host.

Imports the public part of the ssh transfer key onto a remote host. For more information, see [Enabling ssh-key pairs for data archive, data export, data mart](#).

Syntax

```
export-public-transfer-key
```

export remotelog_config

Use this command to propagate either Venafi or remote logging configurations from a central manager to some or all of its associated managed units.

Syntax

```
export remotelog_config < file | scp >
```

Where:

- file - Exports the log to the default Guardium log location.
- scp - Follow the prompts to indicate where you want to store the log.

Examples

```
>export remotelog_config file
Remotelog config exported to /var/IBM/Guardium/log/remotelog_config_202208111122711.json
>export remotelog_config scp
Host: glab-123.mycompany.com
username: hadrian.swall
Full path: /hom/dev/hadrian.swall/test
Warning: Permanently added 'glab-123.mycompany.com, 2.2.2.2' (ECDSA) to the list of known hosts.
hadrian.swall@glab-123.mycompany.com's password:
remotelog_conf_202208111122711
```

export rotated_message_logs

Use this command to export message logs to a remote directory. Each log is created with a unique name.

When you specify this command, Guardium requests the following information:

- Remote host username
- Remote host: The IP address of the remote host
- Remote host directory: The directory for the remote logs.
- Password: The password for the host user (that is, the host username).
- Scp port: To specify a special port, enter it when requested. To use the default port, enter 0 or press Enter.

Syntax

```
export rotated_message_logs
```

fileserver

Use this command to start an HTTPS-based file server running on the Guardium appliance. This facility is intended to ease the task of uploading patches to the unit or downloading debugging information from the unit. Each time this facility starts, it deletes any files in the directory to which it uploads patches.

Note: Any operation that generates a file that the fileserver will access should finish before the fileserver is started (so that the file is available for the fileserver).

Syntax

```
fileserver <IP address> <duration>
```

- **IP address** - Allows access to a specified fileserver. IP address from the local computer you are using is required to retrieve the IP address that is used to bring up the fileserver. If an IP address is not your local computers IP address, the fileserver will not launch.
- **Duration** - Specifies the number of seconds (60 - 3600) to keep the fileserver active. After the specified number of seconds, the fileserver shuts down automatically.

In case of a security setup where browser sessions are redirected through a proxy server, the IP address of the fileserver client will not be the same as the SSH client that started the fileserver. Instead, the fileserver client will have the IP address of the proxy server, and this address must pass the **IP address** parameter. To find the proxy IP address, check your browser settings or the client IP addresses shown in the Logins to Guardium report in the Guardium Monitor interface.

Example

```
fileserver 10.0.0.1 3600
Starting the file server...
The file server is ready at https://guardium.system.com:8445
The timeout has been set to 3600 seconds and it may timeout during the uploading.

The upload will only be accessible from the IP you are logged in from: 10.0.0.1
Press ENTER to stop the file server.
```

Open the fileserver in a browser window, and do one of the following:

- To upload a patch, click Upload a patch and follow the directions.
- To download log data, click Sqlguard logs, navigate to the file you want and download as you would any other file.

When you are done, return to the CLI session and press Enter to terminate the session.

Access VA scripts using fileserver

- From the Guardium CLI, run fileserver <your computer's IP address> 3600.
- Using a browser, go to https://<IP address of your Guardium system>/log/debug-logs/gdmonitor_scripts/.
- Choose the file that matches your database type.

import file

Use this command to import a file.

Select the filetype from the list that displays when you run the command. You can use a wildcard (*) for the file name in the SCP, FTP, and snapshot methods.

Syntax

```
import file
```

For more information, see [backup config](#) and [restore config](#).

import scanner_agent

Import a vulnerability scanner agent. You can import a scanner agent with either SCP or the Guardium fileserver. Guardium supports the following agents:

- Nessus
- Qualys

Syntax

```
import scanner_agent <scp <agent> | sys <agent> <filename>
```

Where:

agent - A supported CVE scanner agent, either *nessus* or *qualys*.

- **scp <agent>** - Follow the prompts to indicate where you want to store the scanner agent.
- **sys <agent> <filename>** - Follow the prompts to indicate where you want to store the scanner agent. Before you import the agent, it must be available on the Guardium fileserver. For more information, see [fileserver](#).

Required information:

- Hostname - The hostname or IP address where the agent resides.
- Username and password - The username and password to log into the host.
- Full filepath - The full path, including the filename of the agent to import, for example, /site/a-support/scanner_tools/agents/NessusAgent/NessusAgent-10.4.2-es8.x86_64.rpm

After you import the agent, then you need to configure it by using the [setup scanner_agent](#) CLI command.

For more information, see [Configuring vulnerability scanner agents](#).

import tsm config

Uploads a TSM client configuration file to the Guardium appliance. You must do this before performing any archiving or backup operations using TSM. You will always need to upload a dsm.sys file, and if that file includes multiple servername sections, you will also need to upload a dsm.opt file. For information about how to create these files, check with your company's TSM administrator.

You will be prompted for a password for the user account on the specified host.

Syntax

```
import tsm config <user@host:/path/[ dsm.sys | dsm.opt ]>
```

Parameters

user@host - User account to access the file on the specified host.

/path/[dsm.sys | dsm.opt] - Full path filename of the file to import.

Note: In setting up TSM on each collector, if the initial configuration fails, a notification error results which says the test file could not be sent. Logging into the collector as root, and then running a dsmc archive command to the TSM server, the TSM file, with the same credentials, now succeeds. Returning to the GUI, and configuring with the same options used before, the configuration now succeeds as well.

If tsm config has passwordaccess=generate, the password stored in a local file, is sought. The root user needs to run the dsmc command once to create this local password file.

After uploading the tsm config file, if tsm config has a passwordaccess generate prompt, passwordaccess is set to be generated.

Would you like to run a dsmc command now to ensure password is set locally (y/n)? If the answer is y, run a "dsmc query options>>/dev/null" command, which will prompt user for password.

import tsm property

Use this CLI command to upload a file to /opt/tivoli/tsm/client/ba/bin/guard_tsm.properties.

The file size should be 1K.

Syntax

import tsm property user@host:file

This command will upload the input file to /opt/tivoli/tsm/client/ba/bin/guard_tsm.properties

restart scanner_agent

Restarts the specified CVE scanner agent.

Syntax

restart scanner_agent <agent>

Where:

agent - A supported CVE scanner agent, either *nessus* or *qualys*.

For more information, see [Configuring vulnerability scanner agents](#).

restore backup

With this command you can restore and upgrade Guardium data files, configuration files, or both from a previously installed system to a newer system. The **restore backup** command does not take any parameters, but provides a series of questions to determine which files you want to restore. In order for the command to work, restore backup needs to be called on the same type of machine on the same patch level.

For any restore, you can select one data backup (DATA) file, one configuration file (CONFIG), or one of each.

The **restore backup** command for CONFIG restores the following configuration information:

- Two-factor authentication configuration
- Authentication credentials for system users
- Universal connector configuration
- Aggregator keys
- CA certificates and repository
- PKI certificates
- Repository of keys and certificates
- Web server configuration and customization
- FIPS enabled/disabled state
- OCR configuration
- Outlier configuration
- Spectrum Protect configuration
- GBDI configuration
- Log rotate configuration

Note: The following data is overridden during a restore:

- User information that is defined by the accessmgr user.
- Information included in export definitions.

When you run **restore backup**, Guardium asks if you want to import backup files and then presents a series of questions to determine their location. Guardium suggests that you import the backup files before you call **restore backup**. Imported files are stored in the /var/dump/ directory.

Note: If you already have backup files on your Guardium system, **restore backup** lists those files. You can either select one of the available files to restore or import different files.

If you choose to import a backup file, then the script requests the following information:

- The file transfer method required for the storage type, such as AMAZONS3, FTP, SCP, SOFTLAYER, or TSM.
- The name of the backup host machine.
- The backup host username.
- The remote directory.

- The remote file to restore. You can use a wildcard (*) to select one or more files. For example, if you know that you want to restore a file from 2022, you can specify 2022* to show all files that include 2022 in the filename. If more than 10 files meet the criteria, Guardium will list up to 10 files at a time. You can select the file you want to import or show the next set of files.
- The password for the user on the host machine.

After you select the files to import and restore and specify the required information, Guardium restores the DATA, CONFIG, or both files to the latest supported version of Guardium.

Note: The restore backup command can only restore files from Guardium V10.1.3 or later. To restore a backup file prior to V10.1.3, first restore it to a V10.1.3 or higher appliance, take a backup from that appliance, then restore the new backup onto the latest release.

Syntax

restore backup

restore config

These commands back up and restore configuration information from the internal administration tables. The backup config command stores data in the /media/backup directory. The backup config command removes license and other machine-specific information. The backup system command provides a more comprehensive backup of the configuration and the entire system.

When restoring a configuration, you must restore a backup that is of the same version and patch level as the original appliance where the backup was created.

Syntax

backup config

restore config

restore keystore

Use this command only under direction from Technical Support.

Use this command to restore certifications and private keys used by the Web servlet container environment (Tomcat).

Syntax

restore keystore

restore pre-patch-backup

Use this command only under direction from Technical Support.

Use this command to recover the pre-patch-backup when the appliance database is up or down.

Syntax

```
restore pre-patchbackup Please enter the information to retrieve the file: Is the file in the local system? (y/n) n Start to
recover with the backup profile parameters. Please check the recovery status in the log
/var/log/guard/diag/depot/patch_installer.log ok ----- If answer 'n', abort the operation. If
answer 'y', need to enter the file name.
```

set up vmware tools

Use this CLI command to install VMware that runs on the ESX infrastructure.

Syntax

setup vmware_tools [install | uninstall]

Step 1: Open the VM client/console and select the VM instance that contains the IBM® Guardium appliance. Right-click the instance, select (from the popup menu) Guest => Install/upgrade VMware tools. This enables the instance to access the VMware tools via a mount point.

Step 2: Run the CLI command (from within the VM client/console), **setup vmware_tools install**, to install VM tools.

setup scanner_agent

Set up a CVE scanner agent.

Syntax

setup scanner_agent <configure | enable | proxy | uninstall> <agent>

Where:

agent - A supported CVE scanner agent, either *nessus* or *qualys*.

- **configure <agent>** - Configure the specified agent that you imported (with the [import scanner agent](#) command), as follows:

For a Nessus agent:

- Linking key - Available from the Tenable Nessus agents dashboard.
- Agent name - Default value is the Guardium system hostname.
- Host - Tenable Nessus system hostname where the agent connects.
- Port - Port number to connect to the Tenable Nessus system.

For a Qualys agent:

- Customer ID - Available from the Qualys agent management dashboard.

- Activation ID - Available from the Qualys agent management dashboard.
- Server URI - Qualys system hostname where the agent connects.
- Proxy host - Proxy hostname, if needed.
- **enable <agent>** - For a Qualys agent, enable the agent after you configure it. Nessus agents start automatically after configuration.
- **proxy <agents>** - If you are using SSL with a proxy, then follow the prompts for your agent to enter proxy information.
- **uninstall<agent>** - Uninstalls the specified agent (*nessus* or *qualys*).

For more information, see [Configuring vulnerability scanner agents](#).

show audit-data

Use this command to display any files that were created by executing the CLI command, export audit-data. For more information about audit data files, see export audit-data.

Syntax

```
show audit-data <yyyy-mm-dd>
```

show scanner_agent

Syntax

```
ca_bundle | configuration <agent> | status <agent> | supported >
```

Where:

agent - A supported CVE scanner agent, either *nessus* or *qualys*.

- **ca_bundle** - Show the certificate information to download with the [store certificate scanner ca_bundle](#).
- **configuration <agent>** - Shows configuration details for the specified agent.
- **status <agent>** - Displays the status for the specified agent.
- **supported** - Displays a list of supported CVE agents.

For more information, see [Configuring vulnerability scanner agents](#).

start scanner_agent

Start the CVE scanner agent.

Syntax

```
start scanner_agent <agent>
```

Where:

agent - A supported CVE scanner agent, either *nessus* or *qualys*.

For more information, see [Configuring vulnerability scanner agents](#).

stop scanner_agent

Stop the CVE scanner agent.

Syntax

```
stop scanner_agent <agent>
```

Where:

agent - A supported CVE scanner agent, either *nessus* or *qualys*.

For more information, see [Configuring vulnerability scanner agents](#).

store language

Initial installation of Guardium is always in English. Use the **store language** CLI command after installation to convert the database from English to the desired language. Setting the desired language is considered part of the initial system set up: changing the language on an established system will impact the information already captured, stored, customized, archived or exported on that system.

Important:

- After switching from English to a desired language, it is not possible to revert back to English using this CLI command. The Guardium system must be reinstalled in English.
- To prevent the system from displaying a mixture of languages, set a central manager and all its managed units to the same language.

Syntax

```
store language
```

Example

```
store language
The following languages are available on this appliance:
 1. French
```

```

2. German
3. Italian
4. Japanese
5. Korean
6. Polish
7. Pseudo
8. Simplified Chinese
9. Spanish
10. Traditional Chinese
Please enter the number of the language you want or 0 to quit:

```

Show command

show language

store tsm authorization

When backupinitiationroot is set to ON in TSM servers, then only root and authorized users can perform backup/archive. When backupinitiationroot is set on and password access in DSM.SYS is set to "generate", Guardium backup and archive to TSM will fail with the error message:

ANS1708E Backup operation failed. Only a root user can do this operation

Non-root users must be authorized to perform backup and archive.

This authorization is enabled by executing the CLI command

Store tsm authorization backupinitiationroot on

This authorization is disabled by executing the CLI command:

Store tsm authorization backupinitiationroot off

Syntax

store tsm authorization backupinitiationroot <on/off>

Show command

show tsm authorization backupinitiationroot <on/off>

This CLI command displays on, if non-root Guardium users are authorized to perform backup and archive when backupinitiationroot is set to ON in TSM servers. Otherwise, it displays off.

Vmware kernel panic after a reboot

VMware ESX 4.1 Virtual machine running Guardium might get a kernel panic after a reboot.

To correct this situation, VMware recommends: Install update 2 on ESX4.1 or Set CPU/MMU virtualization to Use software only instruction set and MMU Virtualization. This option is found under Settings/ Options/ CPU/MMU Use software for instruction set and MMU Virtualization.

Inspection Engine CLI Commands

Use these CLI commands to configure the inspection engines.

An inspection engine monitors the traffic between a set of one or more servers and a set of one or more clients using a specific database protocol (Oracle or Sybase, for example). The inspection engine extracts SQL from network packets; compiles parse trees that identify sentences, requests, commands, objects, and fields; and logs detailed information about that traffic to an internal database.

add inspection-engines

Adds an inspection engine configuration to the end of the inspection engine list. The parameters are described. You can re-order your list of inspection engines after adding a new one by using the reorder inspection-engines command. Adding an inspection engine does not start it running; to start it running, use the start inspection-engines command.

Syntax

add inspection-engines <name> <protocol>

<fromIP/mask> <port> <toIP/mask>

<exclude client list> <active on startup>

Parameters

name - The new inspection engine name; must be unique on the unit.

protocol - The protocol monitored, which must be one of the following: Windows: CouchDB, Db2®, Db2 Exit, Informix®, MongoDB, MS SQL, Mysql, Oracle, PostgreSQL, Sybase; UNIX: Aster, Cassandra, CouchDB, Db2, Db2 Exit, exclude IE, FTP, GreenPlumDB, Hadoop, Hive, HTTP, Hue, IBM® iSeries, Impala, Informix, Informix Exit, Kerberos, MariaDB, MongoDB, Mysql, Netezza®, Oracle, PostgreSQL, SAP HANA, Vertica, Sybase, Teradata, Vertica, or WebHDFS.

fromIP/mask - A list of clients, identified by IP addresses and subnet masks. Separate each IP address from its mask with a slash, and multiple entries by commas. An address and mask of all zeroes is a wild card. If the exclude client list option is Y, the inspection engine monitors traffic from all clients except for those in this list. If the exclude client list option is N, the inspection engine monitors traffic from only the clients in this list.

port - The port or range of ports over which traffic between the specified clients and database servers will be monitored. To specify a range, separate the two numbers with a hyphen.

toIP/mask - The list of database servers, identified by IP addresses and subnet masks, whose traffic will be monitored. Separate each IP address from its mask with a slash, and multiple entries by commas. An address and mask of all zeroes is a wildcard.

exclude client list - A Y/N value; defaults to N. If Y, the inspection engine monitors traffic from all clients except for those identified in the client list. If N, the inspection engine monitors traffic from only the clients listed in the client list.

active on startup - A Y/N value; defaults to N. If Y, the inspection engine is activated on system startup.

delete inspection-engines

Removes the single inspection engine identified by its name. The name can include only letters, numbers and blanks. If the inspection engine name contains any special characters, use the administrator portal GUI to remove it.

Syntax

```
delete inspection-engines <name>
```

reorder inspection-engines

Specifies a new order for the inspection engines, using index values from the list produced by the list inspection-engines command.

Syntax

```
reorder inspection-engines <index>, <index>...
```

Example

If the displayed indices are 1, 2, 3, and 4, the following command will reverse order of the engines:

```
reorder inspection-engines 4,3,2,1
```

restart inspection-core

Restarts the inspection-engine core, but not the inspection engines. The collection of database traffic stops when this command is issued.

12.0 Syntax

```
restart inspection-core
```

12.1 and later Syntax

```
restart inspection-core [--yes]
```

Where --yes causes the command to run automatically.

Note: To restart the collection of traffic for one or more specific inspection engines, follow this command with one or more start inspection engine commands. Alternatively, to restart the collection of traffic for all inspection engines, use the restart inspection-engines command.

restart inspection-engines

Restarts the database inspection engine core and all inspection engines. The collection of database traffic stops temporarily while this occurs and restarts only when database connections re-initiate.

Syntax

```
restart inspection-engines
```

show inspection-engines

Displays inspection engine configuration information, as follows:

all - All inspection engines.

configuration <index> - Only the inspection engine identified by the specified index, which is from the list inspection-engines command.

type <db_type> -Displays configurations of a specific database type, which must be one of the supported monitored protocol types: Windows: CouchDB, Db2, Db2 Exit, Informix, MongoDB, MS SQL, Mysql, Oracle, PostgreSQL, Sybase; UNIX: Aster, Cassandra, CouchDB, Db2, Db2 Exit, exclude IE, FTP, GreenPlumDB, Hadoop, Hive, HTTP, Hue, IBM iSeries, Impala, Informix, Informix Exit, Kerberos, MariaDB, MongoDB, Mysql, Netezza, Oracle, PostgreSQL, SAP HANA, Vertica, Sybase, Teradata, Vertica, or WebHDFS.

Syntax

```
show inspection-engines <all | configuration <index> | log sqlstrings | type <type> >
```

Note: Use the CLI command, show inspection-engines all, to display non-STAP Inspection Engines like SPAN ports. The CLI command, list_inspection_engines, will display inspection engines created by STAP.

start inspection-core

Starts the inspection-engine core.

Syntax

start inspection-core

start inspection-engines

Starts one or more inspection engines identified using index values from the list produced by the list inspection-engines command.

Syntax

start inspection-engines <all | id>

start inspection-engines all

Starts all the inspection engines.

Syntax

start inspection-engine all

start inspection-engines id

Usage: start inspection-engines id <n>, where n is a numeric sniffer id.

Syntax

start inspection-engines id <n>

stop inspection-engines id

Usage: stop inspection-engines id <n>, where n is a numeric sniffer id.

stop inspection-core

Stops the inspection-engine core.

Syntax

stop inspection-core

stop inspection-engines

Stops one or more inspection engines identified using index values from the list produced by the list inspection-engines command. It can also stop all inspection-engines.

Syntax

stop inspection-engine <all | id>

stop inspection-engines all

Stops all the inspection engines.

Syntax

stop inspection-engines all

stop inspection-engines id

Stops one or more inspection engines identified using index values from the list produced by the list inspection-engines command.

Syntax

stop inspection-engine <n>, where <n> is numeric sniffer id

store ignored port list

Sets the complete set of port numbers to be ignored by all inspection engines. The list you specify completely replaces the existing list. Each number is separated from the next by a comma, and no blanks or other white-space characters are allowed in the list. Use a hyphen to specify an inclusive range of numbers.

Syntax

store ignored port list <n>

Example

store ignored port list 33,60-70

Show Command

show ignored port list

Investigation Dashboard CLI Commands

Use these CLI commands to configure the Investigation Dashboard .

show solr connection_timeout

Use this command to show the current connection_timeout value.

```
show solr connection_timeout
```

show solr so_timeout

Use this command to show the current so_timeout value.

```
show solr so_timeout
```

show solr time_allowed

Use this command to show the current time_allowed value.

```
show solr time_allowed
```

store solr connection_timeout

Use this command to set the connection timeout. If the Investigation Dashboard cannot connect to the collector within the specified timeout period, no results from that collector will be returned.

```
store solr connection_timeout [value]
```

| Parameter | Value | Description |
|--------------------|---------|---|
| connection_timeout | integer | The timeout is expressed as a value of 0 to 2147483647 milliseconds.
The default value is 100000 milliseconds. |

store solr so_timeout

Use this command to set the socket timeout.

```
store solr so_timeout [value]
```

| Parameter | Value | Description |
|------------|---------|---|
| so_timeout | integer | The timeout is expressed as a value of 0 to 2147483647 milliseconds.
The default value is 100000 milliseconds. |

store solr time_allowed

Use this command to set the socket timeout.

```
store solr time_allowed [value]
```

| Parameter | Value | Description |
|--------------|---------|--|
| time_allowed | integer | The timeout is expressed as a value of 0 to 2147483647 milliseconds.
The default value is 90000 milliseconds.

Note: Deep search uses 10x (ten times) the time_allowed value. |

Network Configuration CLI Commands

Use the network configuration CLI commands to set IP addresses, handle bonding and failover, handle secondary functionality, and reset networking.

Use the network configuration CLI commands to perform the following tasks:

- Identify a connector on the back of the machine (**show network interface port**).
- Reset networking after you install or move a network card (**store network interface reset**).
- Set IP Addresses (**store network interface ip**, **store network interface mask**, **store network resolver**, **store network routes**).
- Enable or disable high-availability (**store network interface high-availability**).
- Configure the network card if the switch it attaches to does not auto-negotiate the settings (**store network interface auto-negotiation**, **store network interface speed**, **store network interface duplex**).

Guardium uses predictable network interface names. The primary network interface is set during installation and can be changed by using the **store network interface**

`role` command.

restart network

Restarts just the network configuration. For example, change the IP address, then run this CLI command.

12.0 Syntax

```
restart network
```

12.1 and later Syntax

```
restart network [--yes]
```

Where `--yes` causes the command to run automatically.

show network interface all

This command shows settings for the network interface that is used to connect the Guardium® appliance to the desktop LAN. This command displays the IP address, mask, state (enabled or disabled), and high availability status. If IP high-availability is enabled, the system displays two interfaces. Otherwise, only one interface is displayed.

Syntax

```
show network interface all
```

show network interface inventory

Use the show command to display the port names and MAC addresses of all installed network interfaces.

Syntax

```
show network interface inventory
```

Example

```
CLI> show network interface inventory
Current network card configuration:
Device      | Mac Address          | Member of
-----
ens32       | 00:50:56:B8:18:75   |
ens33       | 00:50:56:3b:c3:73   |
ens34       | 00:50:56:8a:0d:fb   |
ok
```

The `Member of` column shows the NICs that are in the bond pair, if a bonding exists.

show network routes operational

Display the IP routing configuration in use.

Syntax

```
show network routes operational
```

Example

```
CLI> show net rout operational
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.3.0 0.0.0.0 255.255.255.0 U 0 0 0 nic1
169.254.0.0 0.0.0.0 255.255.0.0 U 0 0 0 nic2
0.0.0.0 192.168.3.1 0.0.0.0 UG 0 0 0 nic1
ok
```

show network verify

Display the current network configuration.

Syntax

```
show network verify
```

```
CLI> show network verify
Current Network Configuration
```

```
Hostname = test_system.guardium.ibm.com
```

| Device | Address | Prefix | Gateway | Member of |
|--------|---------|--------|---------|-----------|
| ens256 | -- | None | -- | br3 |
| -- | -- | None | -- | -- |
| ens224 | -- | None | -- | br2 |
| -- | -- | None | -- | -- |
| ens160 | -- | None | -- | br0 |
| -- | -- | None | -- | -- |

| | | | | |
|------------------------|----------------------------------|------------|------------|------------|
| ens34 | 9.70.165.96 | 24 | 9.70.165.1 | -- |
| -- | 2002:920:c000:3165:9:70:165:96 | 64 | -- | -- |
| ens192 | -- | None | -- | br1 |
| -- | -- | None | -- | -- |
| Ethtool Options | | | | |
| Device | Options (speed, autoneg, duplex) | | | |
| ens256 | | | | |
| ens224 | | | | |
| ens160 | | | | |
| ens34 | | | | |
| ens192 | | | | |
| DNS Servers | | | | |
| Index | DNS Server | | | |
| 1 | 9.32.193.11 | | | |
| Static Routes | | | | |
| Device | Index | Address | Prefix | Gateway |
| ens34 | 0 | 9.32.145.0 | 24 | 9.32.145.1 |

store network interface auto-negotiation

If auto-negotiation is available on the switch to which a Guardium port is connected, auto-negotiation is used, and only the restart option of this command has any effect. Use this command to enable, disable, or restart auto-negotiation for the specified network interface (NIC). Use **show network interface inventory** to display all port names.

Syntax

```
store network interface auto-negotiation <NIC> <on | off | restart>
```

Show command

```
show network interface auto-negotiation
```

store network interface duplex

Use this command only when auto-negotiation is not available on the switch to which the Guardium port is connected. This command configures duplex mode for the port. Use the **show network interface inventory** command to display all port names.

Syntax

```
store network interface duplex <NIC> <half | full>
```

Show command

```
show network interface duplex <NIC>
```

store network interface high-availability

Enables or disables IP Teaming (also known as bonding), which provides a fail-over capability for the Guardium system primary IP address.

The two ports used (the primary and secondary interfaces) must be connected to the same network. A slight delay might occur if the switch needs to relearn the port configuration. The default setting is off.

When the high-availability option is enabled, the Guardium system automatically fails over, as needed, to the specified secondary interface, which transfers the primary IP address to the secondary interface.

Note: You can specify either IP Teaming and Secondary Interface, but not both.

Syntax

```
store network interface high-availability [on <NIC> [mode <1|4>] | off]
```

If high-availability is enabled, you can optionally specify the NIC mode, which can be:

- 1 - active-backup - Provide fault tolerance features by using an active-backup policy.
- 4 - lacp/802.3ad - Provide load balancing and fault tolerance based on the 802.3ad specification.

store network interface ip

Sets the primary IP address for the Guardium appliance in CIDR (Classless Inter-Domain Routing) format. You might need to change the subnet mask when you change the network interface IP address. For more information, see **store network interface mask**.

See **store network interface secondary** to create and manage a secondary IP address. Bonding or failover is managed from the **store network interface high-availability** CLI command.

Syntax

```
store network interface ip <ip address>
```

store network interface mask

Sets the subnet mask for the primary IP address. If you change the network interface mask, you might also need to change its IP address. See [store network interface ip](#).

Note: The subnet mask for a secondary IP address can be assigned only from [Setup > Tools and Views > System](#).

Note: This command supports IPv4 addresses only.

Syntax

```
store network interface mask <ip mask>
```

store network interface mtu

Use this CLI command to set the maximum transfer unit (MTU).

```
CLI> store network interface mtu
```

Usage: store network interface mtu <interface> <mtu>]

Where *interface* is the interface name (ens32) and *mtu* is the number of transfer units (between 1000 and 9000).

Show command

```
show network interface mtu
```

show network interface port

Use this command to locate a physical connector on the back of the appliance. After you display all port names with [show network interface inventory](#), use this command to flash the light on the physical port specified by NIC (for example, ens32) 20 times.

Syntax

```
show network interface port <nic>
```

Example

```
CLI> show network interface port ens32
```

The orange light on interface ens32 will now blink 20 times.

store network interface reset

Use this CLI command to wipe the existing OS network configuration. This command also detects and builds configuration for the on-board NIC cards within the Guardium appliance.

Syntax

```
CLI> store network interface reset
```

WARNING: This command will clear existing network interface configuration.

Network will be disconnected due to this operation.

Are you SURE you want to continue? (y/n)

store network interface restore

Use this command to restore all of the network settings from your Guardium database settings. Restoring the settings can be useful if, for example, a patch introduces an error into the network configuration. In this case, the information in the database is still correct and you can quickly restore all of your settings.

Note: Static route settings are not saved in the database and are not restored.

Syntax

```
CLI> store network interface restore
```

WARNING: This command will overwrite the network configuration with the stored Guardium network settings.

It may disconnect your current ssh session.

Are you SURE you want to continue? (y/n)

store network interface role

Use this command to assign a role to a physical network interface. A network interface role can be primary, secondary or no role (undefined). Use undefined (`undef`) to clear the role of an interface that is currently set to `secondary`.

Syntax

```
store network interface role <NIC> <undef | primary | secondary>
```

Show command

```
show network interface role
```

store network interface secondary

Use this command to configure a port on the Guardium system as a secondary management interface with a different IP address, network mask, and gateway from the primary.

Note: You cannot use IP Teaming and Secondary Interface at the same time.

Syntax

```
store network interface secondary [on <interface> <ip[/prefix]> <gateway> | off [ipv4|ipv6]]
```

Where

- *interface* is a valid interface.
- *ip* and *gateway* are valid IP addresses.
- */prefix* is the IP address prefix length in CIDR. */prefix* is optional. The default values are 24 for ipv4 or 64 for ipv6.
- *ipv4* and *ipv6* are the IP versions.

Show command

```
show network interface secondary
```

store network interface speed

Use this command only when auto-negotiation is not available on the switch to which the Guardium port is connected. This command configures the speed setting for the port. Use the [show network interface inventory](#) command to display all port names.

Syntax

```
store network interface speed <NIC> <auto | 10 | 100 | 1000>
```

Show command

```
show network interface speed <NIC>
```

show network interface status

Use this command to display the physical link status of a network interface.

Syntax

```
show network interface status <NIC>
```

Example

```
show network interface status ens32
Network Interface Status
    Link detected: yes
ok
```

show network arp-table

Displays the address resolution protocol (ARP) table, which is an operational system value. This command is provided for support purposes only.

Syntax

```
show network arp-table
```

Example

```
CLI> sho net arp
IP address HW type Flags HW address Mask Device
192.168.3.1 0x1 0x2 00:0E:D7:98:07:7F * nic1
192.168.3.20 0x1 0x2 00:C0:9F:40:33:30 * nic1
ok
CLI>
```

show network macs

Displays a list of MAC addresses (like the show network interface inventory command).

Syntax

```
show network macs
```

Example

```
CLI> show network macs
ens32: 00:50:56:b8:18:75
lo: 00:00:00:00:00:00
```

store network resolvers

Sets the IP address for the first, second, or third DNS server to be used by the Guardium appliance. Each resolver address must be unique.

Syntax

```
store network resolvers <IP address 1 [IP address 2] [IP address 3] | null>
```

Enter a maximum of three space-separated IP addresses. To remove the DNS servers, enter null.

Note: This command replaces existing DNS settings.

For example,

- IPv4

```
store network resolvers 192.0.2.0 192.0.2.1 192.0.2.2
This change will take effect after restart network.
ok

• IPv6

store network resolvers 2001:0DB8:0:0:0:0:0:0 2001:0DB8:0:0:0:0:0:1 2001:0DB8:0:0:0:0:0:3
This change will take effect after restart network.
ok

• Dual mode (IPv4 and IPv6)

store network resolvers 2001:0DB8:0:0:0:0:1 192.0.2.0 2001:0DB8:0:0:0:0:3
This change will take effect after restart network.
ok
```

Show command

```
show network resolvers
```

store network routes defaultroute

Sets the IP address for the default router to the specified value.

Syntax

```
store network routes defaultroute <ip address>
```

Show commands

```
show network routes defaultroute
```

store network routes static

Allow the user to have only one IP address per appliance (through the primary interface) and direct traffic through different routers that use static routing tables. Add line to static routing table.

Syntax

```
store network routes static
```

Show command

List the current static routes, with IDs - Device, Index, Address, Netmask, Gateway.

```
show network routes static
```

Delete command

```
delete network routes static
```

store system domain

Sets the system domain name to the specified value.

Syntax

```
store system domain <value>
```

Show command

```
show system domain
```

store system hostname

Sets the system's hostname to the specified value.

Syntax

```
store system hostname <value>
```

Show command

```
show system hostname
```

Support CLI Commands

Use the following CLI commands only under the direction of Technical Support.

These commands are to assist Guardium Technical Support to analyze the status of the machine, troubleshoot common issues, and correct some common problems. You do not need to perform these commands regularly.

store active_parser_engine

This CLI command controls which parser engine that sniffer uses. This CLI command is only applicable to database types supported by ANTLR3 parsers (such as Oracle, Db2, MS SQL, and MySQL).

Syntax

```
store active_parser_engine <num>
```

Where *num* is

- 1 - ANTLR3 parser errors reparsed by ANTLR2 (default)
- 2 - ANTLR2 only
- 3 - ANTLR3 only

Show command

```
show active_parser_engine
```

store antlr3_cached_raw_context_count

Use this command to define how many cached results the sniffer antlr3 parser stores for each raw (prepared) statement map per sniffer thread. The typical workflow for raw statements is that first sniffer receives a raw SQL statement, which is parsed, stored in memory along with its ID, and logged. When sniffer later receives the bind data, the full SQL is reconstructed and reparsed.

With this feature, the cache creates a short-cut where the raw antlr3 parsed result is also stored in memory. It is much faster to retrieve and run the cached statements than having to reparse them on every retrieval. However, the caching also requires much more memory.

The command allows you to specify how many antlr3 raw statement parsed results are cached per sniffer thread, rather than reparsing the reconstructed statements.

Note: The **store antlr3_cached_raw_context_count** function allows the sniffer to process traffic more efficiently when raw statements are heavily used. However, caching the raw statements causes sniffer to consume more memory. It is recommended to enable only the **store antlr3_cached_raw_context_count** function on collectors that have at least 32 GB of memory.

Recommended values are 1000 - 2000 statements per GB of memory. For example, for a 32 GB collector, you can set **store antlr3_cached_raw_context_count** to 32 - 64 (that is, 32,000 - 64,000).

Syntax

```
store antlr3_cached_raw_context_count <num>
```

Where *num* is a number between 0 (disabled) and 1000 (in thousands) or -1 (default) to have sniffer allocate the number of cached results based on the amount of available memory.

Examples

```
store antlr3_cached_raw_context_count 24 - Sets the limit to 24,000.
```

```
store antlr3_cached_raw_context_count 1000 - Sets the limit to 1,000,000.
```

Show command

```
show antlr3_cached_raw_context_count
```

If **store antlr3_cached_raw_context_count** is set to -1, the response is "Available."

store antlr3_max

Use this command to help control data flow between the sniffer parser and logger for either the antlr2 or antlr3 parser.

If the sniffer is running out of memory and restarting, try lowering the antlr3_max logger size. Alternatively, if the sniffer isn't using enough of the available system memory, increase the logger size to allow sniffer to use more system memory.

Note: The **store antlr3_max** command is an advanced parameter for expert users and Customer Support. This command helps control the data flow between parser and logger component of the sniffer for Oracle, Db2, MySQL, or MSSQL.

Syntax

```
store antlr3_max <num>
```

Where *num* is the number of parsed SQL statements that can be processed by the logger queue and can be either:

- A number in the range 1000 - 10000000.
- 0 (the default) - Allows the sniffer to dynamically allocate space based on available memory. For every 500 MB of physical memory, this command allocates space for 1000 parsed SQL statements.

Show command

```
show antlr3_max
```

store antlr3_remove_comments

Use this CLI command to determine whether to log SQL comments in reports and alert messages.

Syntax

```
store antlr3_remove_comments [on | off ]
```

Where:

- *on* - Do not log comments in alerts and reports.
- *off* - Log comments in alerts and reports.

Note: You must restart the inspection engine after you change this command.
Show command

```
show antlr3_remove_comments
```

This command shows whether **store antlr3_remove_comments** is enabled or disabled.

support analyze

Use this CLI command to analyze content.

Parameters

```
support analyze mssql_decryption_config
support analyze sniffer
support analyze tables
support analyze tap_property
support analyze static-tables
```

Analyze the content of static tables by sorting them based on the largest group per value length and value occurrence.

Note: The analyzed reports can be retrieved from the access logs on the file server using the following path: Access logs>opt-ibm-guardium-log>analyze
The following example is a list of analyzed reports in the Guardium access log:

```
analyze_mssql_decryption_config.log
analyze_sniffer_errors.log
analyze_tap_property.log
```

support app_debug

Turns on app_debug for the specified number of minutes.

Syntax

```
support app_debug start
```

At the prompt, enter the number of minutes to run the app_debug function.

support check tables

Invokes the **mysqlcheck -c** command on tables (to check tables for errors). The default table is TURBINE.

Syntax

```
support check tables [dbname [tablename]]
```

Checks run in parallel, so the overall run time can vary. The command shows progress in percentages. All checks time out after 3 minutes. If a check times out, the table name displays after the command completes.

Any errors that are found are stored in the following file.

```
/opt/IBM/Guardium/log/<dbname>_check_tables
```

Where <dbname> is the name of the database that you checked.

Within the <dbname>_check_tables file, for each table that contains an error, the CLI command generates a log file called:

```
check_table_child.<tablename>.<date>.log
```

Where:

- <tablename> - The name of a table with errors
- <date> - Current date

Log files are not generated for healthy tables.

- Specify this command with no parameters to check all tables in TURBINE database.
- Specify *dbname* to check all tables in a specified database. If you do not specify a database, Guardium checks the tables in TURBINE.
- Specify *dbname* and *tablename* to check a single table in the database. Use this command to recheck individual tables where the check timed out. You can use a percent sign (%) as a wildcard in *tablename* parameter.

For example, to search for all tables in TURBINE that begin with the word RULE:

```
support check tables TURBINE RULE%
```

support clean audit_results

A way to manually purge audit results. Use this command only when absolutely necessary to deal with audit tasks that produce a high number of records and take up too much disk space.

Note: Consult with Technical Support before you run this command.

When you run the command, the following steps occur:

1. A Warning message displays and you must confirm that you really want to take this step.
2. This command lists the audit processes and tasks information. It presents the number of rows, ordered from the largest result set to the smallest. The number of report results is greater than or equal to the input value.
3. Select the line number to delete the audit data for the selected process name.

Syntax

```
support clean audit_results <rows>
```

Where *rows* is the number of rows to show. Default = 10.

Note: On a system with many audit tasks, this command can take some time to complete.

support clean log_files

This CLI command deletes the specified file after you confirm the delete. If it cannot find the file, it lists files larger than 10 MB in /var/log and provides a list of large files that you can select for deletion. A warning message is presented and a confirmation step is included.

Syntax

```
support clean log_file <filename>
  >> add filename.
```

support clean centera_files

Guardium archives and backups that are stored within Centera have a deletion date marker that is attached to them by Guardium. However, no facility is available to invoke the deletion. Centera does not have a GUI to allow maintenance of its own files, so it relies on API invocations from client applications.

Use this command to delete marked files within Centera.

Syntax

```
support clean centera_files
```

support clean DAM_data

A way to manually purge database activity monitoring data. Use this command only when absolutely necessary.

Consult with Technical Support before you run this command.

A Warning message and a confirmation step are included in the command.

Syntax

```
support clean DAM_data <purge_type> <start_date> <end_date>
```

Input parameters

purge_type options - agg, exceptions, full_details, msgs, constructs, access, policy_violations, parser_errors, flat_log

start_date - YYYY-mm-dd

end_date - YYYY-mm-dd

support clean hosts

Syntax

```
support clean hosts <IP address> <fully qualified domain name>
```

support clean InnoDB-dumps

Use this CLI command to purge InnoDB tables.

This command is password-protected (for Technical Support only)

Syntax

```
support clean InnoDB-dumps
```

support clean servlets

Deletes *.jsp*.java and *.jsp*.class files and restarts GUI.

Use this CLI command to delete generated Java™ servlets and their classes.

Syntax

```
support clean servlets
```

[support dump_gdm_exception_error](#)

Dumps GDM_ERROR and GDP_EXCEPTION tables to the Guardium log file location.

12.0 Syntax

```
support dump_gdm_exception_error
```

12.1 and later Syntax

```
support dump_gdm_exception_error [--yes]
```

Where --yes causes the command to run automatically.

[support execute](#)

This utility is designed to provide Guardium Advanced Support with the ability to assist with remote diagnostics and support when direct remote access is not available or permitted.

The **support execute** command is not a replacement for direct remote connections, but allows Guardium Support at least some level of root access in a secure way without direct access.

The commands that are provided by Guardium Advanced Support can be SQL statements, O/S Commands, Shell Scripts, or SQL scripts. The scripts are provided to the customer along with a Secure Key to allow the command to run using the CLI. The Secure key is tied to the system that Guardium Support is working on with the customer, and is not valid for any other system. The command can only be run the number of times that are permitted by Guardium Support and is only valid for seven days from the agreed date.

The feature is disabled by default. Enable it using the CLI command in either normal and recovery mode.

Syntax

```
support execute [enable | disable]
```

To permit the Guardium Advanced Support team to generate a Secure Key, the MAC address of the system in question must be provided for ens32.

Examples:

```
support execute <CMD String> <PMR #> <KEY>
```

main execute command provided by Guardium Advanced Support.

```
support execute showlog [<Secure Key>|main|files]
```

Show usage logs
'<Secure Key>' for full details of single entry
'main' to display the main execute log
'files' to display log directory list

```
support execute mac
```

ens32 MAC address required by support to generate secure key

```
support execute info
```

Show ens32 MAC address, root passkey & other system information

```
support execute version
```

Display the "Support Execute" internal binary code version

```
support execute help
```

Help details and purpose of utility information

Example of command provided by Guardium Advanced Support:

```
support execute "select * from GDM_ACCESS%5CG" 11111,111,111 6254130c0f0c3c504b33687c57f41363e4c00
```

[support gather_io_metrics](#)

This command manages the **gather_io_metrics** service to collect information about I/O statistics on the Guardium appliance when you run the command. With the **start** parameter, this command creates a **gather_io_metrics.txt** file. In addition, Guardium includes the **gather_io_metrics.txt** file with the output of any **must_gather** command. For more information, see [support must_gather commands](#).

Syntax

```
support gather_io_metrics [remove_log | start | status |stop]
```

Where:

- **remove_log** - Delete the current **gather_io_metrics.txt** file.
- **start** - Start to gather I/O metrics. By default, the service runs for 24 hours, unless you stop it sooner.
- **status** - Provide the current status of the **gather_io_metrics** service. Reports on **iostat** command output, whether the service is running, and other information.
- **stop** - Stops the **gather_io_metrics** service.

[support get_gdp_cluster_info](#)

This command gathers information about your Guardium® Data Protection environment to help you, and your support contact, determine the size required for a Guardium Insights cluster. Run the command on a central manager.

Syntax

```
support get_gdp_cluster_info
```

The data is sent to the Guardium fileserver at /opt/IBM/Guardium/log/gdp_cluster_info.csv. The .csv file displays a row for each managed collector that contains the following information:

- LAST_PING_DATE
- UNIT_HOST_NAME
- SQLGUARD_VERSION
- LAST_INSTALLED_PATCH
- DATA_PURGE_AGE
- MEMORY_SIZE
- CPU_CORES
- VAR_SPACE
- DB_SIZE
- NUMBER_OF_DATABASES
- SESSION_LINES
- SESSION_AVG_LINE_LENGTH
- INSTANCE_LINES
- INSTANCE_AVG_LINE_LENGTH
- POLICY_VIOLATIONS_LINES
- POLICY_VIOLATIONS_AVG_LINE_LENGTH
- EXCEPTION_LINES
- EXCEPTION_AVG_LINE_LENGTH
- FULL_SQL_LINES
- FULL_SQL_AVG_LINE_LENGTH
- VA_LINES
- VA_AVG_LINE_LENGTH
- CLASSIFIER_LINES
- CLASSIFIER_AVG_LINE_LENGTH

After you run the command, retrieve the gdp_cluster_info.csv from the Guardium fileserver and send it to Guardium Insights support for analysis.

support logrotate message

By default, log files rotate weekly and store the four most recent log files. Use this command to change the log rotation strategy for the log files.

Syntax

```
support logrotate message [frequency] [# of rotations] [# of steps]
```

Where:

- *frequency* - The frequency with which to rotate the files. Frequency can be one of *hourly* / *daily* / *weekly* / *monthly*.
- *# of rotations* (integer) - The number logs to keep. The default is 4. After Guardium reaches the specified number of logs, the oldest log is deleted. The following example rotates the logs every week and stores the three most recent logs:

```
support logrotate message weekly 3
```

- *# of steps* (integer) - The number of steps (an hour, day, week, or month) to skip in the specified frequency. The following example stores the five most recent logs and rotates the logs every second day:

```
support logrotate message daily 5 2
```

Show command

```
support show logrotate message
```

support must_gather commands

As the CLI user (that is, the user named CLI), you can run must_gather commands to generate specific information about the state of most Guardium systems. After you run the command, upload this information from the appliance and send it to Guardium Technical Support whenever a PMR (Problem Management Record) is logged.

The CLI user can run the must_gather commands at any time, as follows.

1. Open a PuTTY session (or similar) to the Guardium system of concern.
2. Log in as user *cli*.
3. Depending on the type of issue you are facing, enter the relevant must_gather commands into the CLI prompt in the following format.

Syntax

```
support must_gather <arg>
```

Where *arg* is a single must_gather command. You might need more than one must_gather command to diagnose the problem.

- **agg_issues** - Aggregation process issues.
- **alert_issues** - Alerting issues.
- **app_issues** - Application issues.
- **audit_issues** - Audit process issues.
- **auth_issues** - Authentication issues (including LDAP and multifactor authentication).
- **auto_create_ie** - Auto create inspection engines issues.

- **backup_issues** - Backup process issues.
- **big_data_issues** - Big data issues.
- **cm_issues** - Central manager issues.
- **compliance_mon_issues** - Compliance monitoring issues.
- **datamining_issues** - Data mining issues.
- **datastreams_issues** - Data streaming issues.
- **deploy_agents_issues** - Deployment agents issues.
- **deployment_issues** - Deployment issues.
- **eagle_eye_issues** - Advanced threat scanning issues.
- **enterprise_load_balancer_issues** - Enterprise load balancer issues.
- **entitlement_issues** - Entitlement optimization issues.
- **go_stream** - Go stream issues.
- **jproxy_issues** - Jproxy issues.
- **miss_dbuser_prog_issues** - System database user issues.
- **native_auditing_issues** - Native auditing issues.
- **network_issues** - Network architecture issues.
- **patch_install_issues** - Patch installation and upgrade issues.
- **purge_issues** - Purge process issues.
- **risk_spotter** - Risk spotter issues.
- **scanner_agent_issue**
- **scheduler_issues** - Scheduler issues.
- **slon_looper** - Slon looper output.
- **sniffer_issues** - Sniffer issues.
- **system_db_info** - Guardium system database or operating space performance issues.
- **universal_connector_issues** - Universal connector issues.

The following commands might take a few minutes to complete.

- **support must_gather miss_dbuser_prog_issues**
- **support must_gather sniffer_issues**

For the following commands, you are prompted for a time (in minutes) for how long you want to run the debugger to reproduce the problem.

- **support must_gather backup_issues**
- **support must_gather scheduler_issues**

Guardium writes the output to the must_gather directory with filenames, for example:

```
must_gather/system_logs/.tgz
```

4. Send the resulting output to IBM® Support.

Use the **fileserver** CLI command to upload the tgz files and send to them to support.

Send the output in an email or upload to ECUREP in, for example, the standard data upload specifying the PMR number and file to upload.

To purge must_gather files from the Guardium system, see [show must_gather file max age](#).

support must_gather datamining_issues

Collects necessary diagnostic information for Outliers, Quick search and data mart functionality. Information includes dumps of corresponding internal tables, necessary logs, state of corresponding processes, and standard must_gather diagnostics (general system and internal DB information).

Syntax

```
support must_gather datamining_issues
```

support must_gather network_issues

The command gathers all network information from the appliance and polls hosts that Guardium interacts with by using ping, traceroute, corresponding port probing, and other measures. If the optional parameter is specified, then it polls only the host that was specified (if Guardium is configured to do any activity on this host).

Syntax

```
support must_gather network_issues [--host=<HOST>]
```

Where optional parameter --host is the hostname or IP address.

support reset-managed-cli

Use this command from a central manager to login to each associated managed unit and set the CLI passwords and expirations to match the passwords and expiration dates as the central manager.

For this procedure to work, the root passkey must be set on each managed unit. For more information, see [Resetting the root password](#).

Syntax

```
support reset-managed-cli
```

support reset-password

This command resets a password on the IBM Guardium appliance. For root and cloudsupport accounts, only use this command when requested to do so by IBM Technical Support.

Syntax

```
support reset-password [ accessmgr | cloudsupport | root ]
```

Where:

- **accessmgr** - Resets the accessmgr password.
If the accessmgr email is set up, the system notifies the accessmgr account email.
- **cloudsupport** - For cloud images only, resets the password for the cloudsupport account.
The cloudsupport password uses a joint password mechanism for security. Your site holds the keys to the appliance in the form of an encoded numeric passkey. IBM holds the passkey decoder.

When you call Guardium support, the support analyst will start a remote desktop sharing session and request the cloudsupport passkey for the Guardium appliance in question. Guardium support uses the cloudsupport password to gain access to the appliance as cloudsupport user.

Use this command to reset the password key and **support show passkey cloudsupport** to view the passkey.

- **root** - Resets the root password on the IBM Guardium appliance.
This command requires that you provide a secret keyword in order to change the root password. Contact Technical Support if you need to change the root password.

Note: Do not reset the root password unless required by business rules.

support schedule find_crashed_tables

Use this CLI command to enable or disable the daily cron job of find_crashed_tables.sh script.

Syntax

```
support schedule find_crash_tables on ALL|db  
support schedule find_crash_tables off
```

This command enables or disables the daily schedule of find_crashed_tables script.

Note: Pay particular attention to the database entered. Enter "ALL" in order to process all five valid databases for crashed tables or just one of the five valid databases "TURBINE", "GDMS", "CUSTOM", "DATAMART" or "DIST_INT".

support server

The support server is an advanced diagnostic utility that generates a summarized report of your Guardium system.

Use the **support server** command to list all of the support server CLI commands.

Run this command to enable the support server on your Guardium system.

```
support server enable
```

Run this command to disable the support server on your Guardium system.

```
support server disable
```

Use this command to get a summarized report of your Guardium system.

```
support server info
```

support show boot check

Use this command to perform a health check on the boot order of kernels in the boot loader. If the boot order has not been customized and the latest kernel version is not the first entry in the boot order, the command returns **Failed**. Otherwise, the command returns **Passed**. If the boot order has been customized, the command always returns **Passed**.

support show boot order

Use this command to display the boot order of kernels in the boot loader.

support show db-processlist

This command lists all of the database processes sorted by running time.

Syntax

```
support show db-processlist all  
support show db-processlist locked  
support show db-processlist running  
support show db-process full
```

Parameters:

```
support show db-processlist [ ]
```

Where:

- *all* - Includes sleeping processes
- *full* [optional] - Displays SQL queries in expanded format
- *locked* - Displays all locked processes
- *running* - View all running SQL statements

support show db-struct-check

This command displays all the structure differences that are found during aggregation process.

Syntax

```
support show db-struct-check
```

support show db-top-tables

This command lists the 20 largest database tables sorted by size and lists tables sorted by used free table space for tables that use more than 80% free space. It allows filtering by table name. All table sizes are displayed in MB, free space usage in percentage.

Syntax

```
support show db-top-tables all
```

```
support show db-top-tables like
```

Parameters

```
support show db-top-tables all
```

Lists the largest tables out of the entire database sorted by size.

```
support show db-top-tables like
```

Lists the largest tables by matching criteria, which can be any portion of the table name.

support show db-status

This command shows database usage.

Parameters are *free*, *used*, *megabytes*, *percentage*.

Syntax

```
support show db-status free %
```

```
support show db-status used %
```

```
support show db-status free m
```

```
support show db-status used m
```

support show hardware-info

This command uses a script to collect hardware information and places this collected information in a directory for retrieval.

After running this CLI command, the following message displays:

```
Collected HW Info as /var/log/guard/Gather_hw_info-2012-06-25-17-43.tgz
```

Then run the **fileserver** CLI command to retrieve this .tar file from the server.

support show innodb-status

Use this CLI command to troubleshoot MySQL issues. Use this CLI command to check what is happening at runtime with MySQL tables. Use this CLI command to determine if long check times with MySQL tables are due to record lock or table lock.

Syntax

```
support show innodb-status
```

```
0 queries inside InnoDB, 0 queries in queue
0 read views open inside InnoDB
Main thread process no. 7959, id 139923805550336, state: sleeping Number of rows inserted 6894, updated 6934, deleted 93, read 2478'
-----
END OF INNODB MONITOR OUTPUT
```

support show iptables

This command displays the output of system iptables command.

Syntax

```
support show iptables diff
```

```
support show iptables list
```

Parameters

[diff | list] parameter controlling normal iptables output presentation versus displaying only differences/delta.

[accept | full] parameter filters output by accept row versus an unfiltered list.

support show large_files

This command lists all the files larger than <size> and older than <age> in the /var /tmp /root folders.

Syntax

```
support show large_files
```

This command lists all the files larger than MB and older than days in the /var /tmp /root folders.

Input parameters:

- * size - integer > 10 (in MB)
- * age - integer >= 0 (in days)

Syntax:

```
support show large_files <size> <age>
```

Where:

- size - The minimum size files to display (default 100M).
- age - The number of days since the last modification.

show must_gather_file_max_age

Use this command to change the number of days that a must_gather file is stored in the Guardium system before purging.

Syntax

```
store must_gather_file_max_age <num days>
```

Where the value for num days is any integer greater than 1 and the default value is 30.

The file **cleanup_must_gather_files.log** logs all the files that are purged by the **store must_gather_file_max_age** command.

support show netstat

This command displays the output of system netstat command. It allows filtering of the output by content using a grep parameter.

Syntax

```
support show netstat [ all | grep ]
```

Where:

- all - Shows the output of the system netstat command.
- grep - An alphanumeric string to search. The command returns the output that matches the search parameters.

support show passkey

This command displays a passkey that you created using the **support reset-password** command.

Syntax

```
show passkey < accessmgr | cloudsupport | root |
```

Where,

- *accessmgr* shows the passkey for the accessmgr.
- *cloudsupport* shows the passkey for cloud images, such as Azure, IBM Cloud, or Oracle OCI. Use **show passkey cloudsupport** to show the passkey (access key) that Guardium technical support requires to access a cloud image during a support call.
- *root* shows the passkey for the current (non-cloud) appliance. Use this command to show the passkey that Guardium technical support requires to access the appliance if you are locked out of root.

For more information, see [support reset-password](#). For more information about the root password, see [Resetting the root password](#).

support show port open

This command is similar to using telnet to detect an open TCP port locally or on a remote host.

If we are able to connect successfully, a message similar to the following displays:

```
Connection to 127.0.0.1 8443 port [tcp/*] succeeded!
```

If you are unable to connect, a message similar to the following displays:

```
Connect to 127.0.0.1 port 1 (tcp) failed:  
Connection refused
```

Syntax

```
support show port open
```

IP port - IP must be a valid IPv4 address (such as 127.0.0.1).

Port must be an integer with a value in 1-65535.

support show top

This command displays the output of system top command sorted by cpu, memory or running time. You can specify the number of iterations (default =1) and number of displayed rows (default =10).

Syntax

```
support show top [ cpu | memory | time ]
```

Parameters

- **CPU <N> <R>**
- **memory <N> <R>**
- **time<N> <R>**

Where *N* is number of iterations (between 1 and 10) and *R* is number of rows to display (minimum = 10).

support store boot custom

Use this command to manually define (customize) the first kernel entry in the boot loader. Use **support store boot custom** to show all installed kernels and the corresponding index value, then use the index value to define the first kernel entry in the boot loader. Use **support store boot custom off** to turn off boot loader customizations.

Syntax

```
support store boot custom [ <index> | off ]
```

support store boot sanitize

Use this command to reorder the kernels in boot menu. If the boot order has not been customized, the command sorts all currently installed kernels in descending order by version. If the boot order has been customized, the command does nothing.

Syntax

```
support store boot sanitize
```

support store datastreams_diag

Turn data stream debug level logging off or on. When logging is on, datastream logs are stored in ..//opt/IBM/Guardium/log/datastreams.

Syntax

```
support store datastreams_diag [ off | on ]
```

support store hosts

The **support store hosts** command appends an IP-address/domain-name pair to the operating system hosts file (/etc/hosts). The hosts file translates hostnames to IP addresses.

Syntax

```
support store hosts <IP_address> <fully_qualified_domain_name>
```

Example

```
support store hosts 1.2.3.4 mydomain.company.com
```

This example adds the following line to the end of the hosts file:

```
1.2.3.4 mydomain.company.com # CREATED BY CLI, DO NOT CHANGE
```

Show command

```
support show hosts
```

This command shows entries added to the /etc/hosts file using the **support store hosts** command.

support store ora_tns_errors

Controls handling of TNS errors early in processing, giving the option to not log them at all.

Syntax

```
support store ora_tns_errors [0 | 1]
```

- 0 - Do not store TNS errors
- 1 - Store TNS errors (default)

Show command

```
support show ora_tns_errors
```

[support store rdsdiag](#)

Manage Amazon Web Services (AWS) relational database service (RDS) monitoring.

12.0 Syntax

```
support store rdsdiag < clean | off | on >
```

where:

- *clean* - Attempts to delete all core dumps older than 3 minutes from /var/tmp/rds.
- *off* - When RDS monitoring is on, turn on RDS diagnostics.
- *on* - When RDS monitoring is on, turn off RDS diagnostics.

12.1 and later Syntax

```
support store rdsdiag < clean [--yes] | off | on >
```

- *clean* - Attempts to delete all core dumps older than 3 minutes from /var/tmp/rds.
Where --yes causes *clean* to run automatically.
- *off* - When RDS monitoring is on, turn off RDS diagnostics.
- *on* - When RDS monitoring is on, turn on RDS diagnostics.

For more information about turning on RDS monitoring, see [start rds monitoring](#).

[support store snif_auto_hostname_cache](#)

Use this command to toggle sniffer hostname caching.

Syntax

```
support store snif_auto_hostname_cache [ on | off ]
```

Where:

- *on* - Sniffer automatically detects and caches hostnames.
- *off* - Use CLI commands to control hostname caching.

Show command

```
support show snif_auto_hostname_cache
```

[support store snif_auto_os_name_cache](#)

Use this command to toggle sniffer operating system name caching.

Syntax

```
support store snif_auto_os_name_cache [ on | off ]
```

Where:

- *on* - Sniffer automatically detects and caches operating system names.
- *off* - Use CLI commands to control operating system caching.

Show command

```
support show snif_auto_os_name_cache
```

[support store snif_auto_service_name_cache](#)

Use this command to toggle sniffer service name caching.

Syntax

```
support store snif_auto_service_name_cache [ on | off ]
```

Where:

- *on* - Sniffer automatically detects and caches service names.
- *off* - Use CLI commands to control service caching.

Show command

```
support show snif_auto_service_name_cache
```

[support store snif-debug](#)

Use this command to turn the snif debug on or off.

Syntax

```
support store snif-debug [on | off]
```

Show command

```
support show snif-debug
```

support store snif_dump_invalid_msgs

Use this command to control the maximum number of invalid TAP messages that snif will write to a log file in a 5 minute period.

Syntax

```
support store snif_dump_invalid_msgs [ off | on | rate_limit | size_limit ]
```

Where:

- *off* - Do not write invalid messages to the log file.
- *on* - Write all messages to the log file, regardless of whether they are valid.
- *rate_limit <num-msgs>* - Sets the maximum number of invalid TAP messages that are written to the log file in a 5-minute period, where *num-msgs* is 0 or greater.
- *size_limit <file-size-mb>* - Sets the maximum file size for the snif log file containing invalid TAP messages. *file-size-mb* is the file size is between 1 and 4000, in MB.

Show command

```
support show snif_dump_invalid_msgs
```

support store snif_hostname_cache

Use this command to manage either IPv4 or IPv6 IP addresses cached for the sniffer hostname.

Syntax

```
support store snif_hostname_cache [ remove | set ]
```

Where:

- *remove <IP>* - Removes an IP address from the operating system name entry.
- *set <IP>* - Sets the IP address for a hostname entry. This command overwrites any existing entries.

Show command

```
support show snif_hostname_cache [ all | search ]
```

Where:

1. *all* - Show all cached hostname entries.
2. *search* - Enter a set of characters to search on (such as all or part of an IP address or hostname).

support store snif_memory_max

Syntax

```
support snif_memory_max <num>, where num is a number of | 33 | 50 | 75 |
```

This command applies to 64-bit systems only.

Show command

```
support show snif_memory_max
```

support store snif_os_name_cache

Use this command to manage either IPv4 or IPv6 IP addresses cached for sniffer operating system name.

Syntax

```
support store snif_os_name_cache [ remove | set | upload ]
```

Where:

- *remove <IP>* - Removes an IP address from the operating system name entry.
- *set <IP>* - Sets the IP address for an operating system name entry. This command overwrites any existing entries.
- *upload <file>* - Uploads one or more operating system name entries. The file name must be *os.arc.upload*, the first line is the number of operating system name entries in the file, each subsequent line contains the IP address and an OS name, separated by a space. For example:

```
2
192.168.1.100 test1.domain.com
192.168.1.101 test2.domain.com
```

Show command

```
support show snif_os_name_cache [ all | search ]
```

Where:

1. *all* - Show all cached operating system name entries.
2. *search* - Enter a set of characters to search on (such as all or part of an IP address or operating system name).

support store snif_service_name_cache

Use this command to manage either IPv4 or IPv6 IP addresses cached for sniffer service names.

Syntax

```
support store snif_service_name_cache [ remove | set ]
```

Where:

- *remove <IP>* - Removes an IP address from the service name entry.
- *set <IP>* - Sets the IP address for a service name entry. This command overwrites any existing entries.

Show command

```
support show snif_service_name_cache [ all | search ]
```

Where:

1. *all* - Show all cached service name entries.
2. *search* - Enter a set of characters to search on (such as all or part of an IP address or service name).

support store slon

Turns on SLON utility that captures packets gotten by sniffer for debug. Results files slon_packets.tar.gz, slon_messages.tar.gz or slon_all.tar.gz can be found using the **fileserver** CLI command. The /var partition must have at least 15GB of free space.

Syntax

```
support store slon [ on [parameter] | off [parameter] ]
```

Where:

- *on* - Turns the SLON utility on. You can specify the following optional parameters:
 - *packets* - Dump analyzer packets (default)
 - *snifsql* - Log sniffer SQL activities and dump analyzer packets
 - *secparams* - Log secure parameters information and dump analyzer packets
 - *sgate* - Log S-GATE debugging info and dump analyzer packets
 - *messages* - TAP message data dump
- *off* - Turn the SLON utility off. You can specify one of the following parameters:
 - *packets* - Stop dumping packets, logging secure parameters, S-GATE debug info and sniffer SQL activities (default)
 - *messages* - Stop TAP message data dump
 - *all* - Stop all activities

Show command

```
support show slo
```

support store tcpdump

Turns on TCPDUMP utility. After period ends, results file tcpdump.tar.gz can be found with the **fileserver** CLI command. The /var partition must have at least 15GB of free space.

Syntax

```
support store tcpdump [ on <type> <period> <loglimit> [interface] [IP] [port] [protocol] | off ]
```

Where:

- *on* - Turns TCPDUMP utility on. Specify the following parameters:
 - *type* - Dump type:
 - 'headers' - Capture headers only
 - 'raw' - Capture whole packets
 - *period* - Dump period, NUMBER[SUFFIX], where optional SUFFIX can be 's' for seconds, 'm' for minutes (default)
 - *loglimit* - Dump logfile limit, from 1 to 6 gigabytes
 - Optional filter arguments:
 - *interface* - Network interface name (default the primary interface)
 - *IP* - IP address
 - *port* - Port
 - *protocol* - Protocol, which can be one of: 'tcp', 'udp', 'ip', 'ip6', 'arp', 'rarp', 'icmp' or 'icmp6'
- *off* - Turns the TCPDUMP utility off. After stopping, the results file tcpdump.tar.gz can be found using the **fileserver** CLI command.

Example

```
support store tcpdump on headers 10m 1
```

This command runs TCPDUMP saving packets headers for 10 minutes and 1GB log file size limit.

Show command

```
support show tcpdump
```

support store zdiag

Toggles the Guardium for z/OS traffic diagnostics on or off. This includes collection of TCPDUMP and SLON, collections stop when corresponding files reach 2 GB size. After completion, the results files tcpdump.tar.gz and slon_all.tar.gz can be found using the **fileserver** CLI command. The /var partition must have at least 15GB of free space.

Syntax

```
support store zdiag [ on [N] | off ]
```

Where:

- **on** - Turns zdiag on. *N* (optional) is number of minutes to run diagnostics, from 10 to 600, 60 by default.
- **off** - Turns zdiag off.

Show command

```
support show zdiag
```

System CLI Commands

Use these CLI commands to view and configure system settings.

show openssh version

Shows the OpenSSH version of the Guardium system.

Syntax

```
show openssh version
```

show openssl version

Shows the OpenSSL version of the Guardium system

Syntax

```
show openssl version
```

show os version

Shows the operating system version of the Guardium system.

Syntax

```
show os version
```

start ecosystem

Use this command to restart the entire set of ecosystem processes. This restart is necessary after you install patches, run upgrades and some other operations.

Syntax

```
start ecosystem
```

stop ecosystem

Use this command to temporarily and gracefully stop the entire set of ecosystem processes. You need to stop the ecosystem for patching, upgrades and some other operations.

Syntax

```
stop ecosystem
```

store allow_reinstall

When you install Guardium from CD or DVD media, due to host server settings, the media is not always ejected correctly. In this case, when the system is rebooted, it can cause the system to keep reinstalling from the media, rather than rebooting only.

During a reboot, the installer searches the disk to see whether the requested version of Guardium is already installed. If it is installed, and **allow_reinstall** is set to *off*, Guardium pauses to prompt whether to continue the installation process (or reboot only without reinstalling). For example:

```
"Already installed 11.3.0, continue to reinstall (c) or reboot with any other key: "
```

In this case, click *c* to reinstall, or any other key to reboot.

If **allow_reinstall** is set to *on*, the system reinstalls from the media without prompting.

Tip: If **allow_reinstall** is set to *off* (the default) and the installer prompts you to reinstall, the media has a problem. Manually eject the CD or DVD before rebooting.

Syntax

store allow_reinstall [on | off]

The default is *off*.

Show command

show allow_reinstall

store system apc

Use this command to configure automatic powering down options when a UPS is attached. The UPS must be attached to a USB connector (serial connections for a UPS are not supported).

Sets the minimum charge percent (0-100) before powering down, or the number of seconds to run on battery power before powering down. The defaults are 25 (percent) and zero (seconds).

The following commands start and stop the apc process. The apc process is disabled by default.

Syntax

store system apc [battery-level <percent> | timeout <seconds>]

store system apc start

store system apc stop

Show command

show system apc [battery-level | timeout]

store system auditlog-passthrough

Use this command to enable or disable the passing-through of system audit log data from the auditd service to the local syslog. Because the system audit log is verbose, the **auditlog-passthrough** feature is best used along with remote logging. For more information about remote logging, see [Configuration and control CLI commands](#).

The **auditlog-passthrough** feature is disabled by default.

Syntax: **store system auditlog-passthrough [on | off]**

Example:

```
> store sys aud on
Restarting auditd service to pick up the change.
Reloading configuration: [ OK ]
Auditd to syslog passthrough is enabled.
ok
```

Show command: **show system auditlog-passthrough**

store system banner

Use this CLI command to create a banner at the CLI login. You can use the banner to create your own welcome message, warn about unauthorized access, or provide other useful information.

store system banner [message | clear | default]

Syntax

store system banner clear: Remove an existing banner message.

store system banner message: Create a banner message. Enter the banner message and then press CTRL-D.

store system banner default: Reset the banner to the default message.

Show command

show system banner

store system classifier profile

Use this command to adjust the memory available for classification.

Syntax

store system classifier profile [default|small|medium|large|max]

Where the profile values are not exact, but map to the following approximate sizes:

- **default** - 4 GB (same as large)
- **small** - 1 GB
- **medium** - 2 GB
- **large** - 4 GB

- **max** - 8 GB

Show command

show system classifier profile

store system clock datetime

Use this CLI command to set the system clock's date and time to the specified value.

Syntax

store system clock datetime <YYYY-mm-dd hh:mm:ss>

Where:

- *YYYY* - year
- *mm* - month
- *dd* - day
- *hh* - hour (in 24-hour format)
- *mm* - minutes
- *ss* - seconds.

The seconds portion is required, but is always set to 00.

Show command

show system clock <all |datetime |timezone>

Example

```
store system clock datetime 2018-10-03 12:24:00
```

store system clock timezone

Use this CLI command to list the allowable time zone value (list option), or set the time zone for this system to the specified time zone. Use the list option first to display all available time zones, and then enter the appropriate time zone from the list.

IBM® Guardium® also logs the local time zone in the standard audit trail to address cases where data is used in (or aggregated with) data that is collected in other time zones.

Syntax

store system clock timezone <list | timezone>

Show command

show system clock <all | timezone | datetime>

Example

Use the command first with the *list* option to display all available time zones. Then enter the command a second time with the appropriate zone.

```
CLI> store system clock timezone list
Timezone:          Description:
-----
Africa/Abidjan:
Africa/Accra
Africa/Addis_Ababa:
...
...output deleted
...
CLI> store system clock timezone America/New_York
```

store system conntrack

This CLI command sets the current status of the connection tracking subsystem of the Linux® kernel.

Syntax

store system conntrack <ON|OFF>

Show command

show system conntrack

store system cpu profile

Allow configuration of CPU scaling from a CLI command on hardware that supports CPU scaling.

Use this CLI command to set the appropriate CPU scaling policy for your needs:

- **conservative** - Less power usage, conservative scaling
- **balanced** - Medium power usage, fast scale up
- **performance** - Runs the CPUs at maximum clock speed

Guardium software sets the scaling policy to Performance upon installation.

Syntax

store system cpu profile [min|perf|max]

Show command

show system cpu profile

store system custom_db_size

Use this CLI command to set the maximum size of the custom database table (in MB). The Default value is 4000 MB.

Syntax

```
CLI> store system custom_db_max_size  
USAGE: store system custom_db_max_size <N>  
      where N is number larger than 4000.
```

Show command

show system custom_db_size

store system domain

Sets the system domain name to the specified value.

Syntax

store system domain <value>

Show command

show system domain

store system fipsmode

Use this command to enable or disable Federal Information Processing Standard (FIPS) cryptographic standards.

Syntax

store system fipsmode [on | off]

Note: Restart your system after enabling or disabling FIPS mode for the changes to take effect.

Show command

show system fipsmode

store system hostname

Sets the system's hostname to the specified value.

Syntax

store system hostname <value>

Show command

show system hostname

store system ipmode

Use this command to change the IP (Internet Protocol) mode of your Guardium system. For more information, see [Internet Protocol modes](#).

Syntax12.0

store system ipmode[ipv4|ipv6|dual]

Syntax12.1 and later

store system ipmode[ipv4|ipv6|dual] --{yes}

Where --yes causes the command to run automatically

Show command

show system ipmode

store system issue

Use this CLI command with the message parameter to receive input from the console until CRTL-D and write it to /etc/motd after removing from the input any \$,\, followed by single letter, and ` characters. Use this command to enter messages that make this system compliant with the security policies of customers.

Use this CLI command with the clear parameter to restore /etc/motd to the default version.

store system issue [message | clear]

Note: The version comes from /etc/guardium-release. For example, SG70 refers to 7.0, SG80 refers to 8.0. If the SG is not found in /etc/guard-release, the default version is an empty string.

store system netfilter-buffer-size

Use this CLI to set the maximum number of packets the kernel netfilter queue stores internally before dropping upcoming packets. The value is stored in an internal Sniffer configuration table.

Note: Do not use this command without consulting Guardium support.

Syntax

store system netfilter-buffer-size

Show command

Displays the S-TAP® netfilter buffer size. The default is 65536 packets.

show system netfilter-buffer-size

store system patch

The parameters for this command are cleanup, and install.

Store system patch cleanup

Deletes the patches that are selected from an itemized list.

Example:

```
> store system patch cleanup
Patches:
1. SqlGuard-11.Op118.tgz.enc.sig
2. SqlGuard-11.Op121.tgz.enc.sig
3. SqlGuard-11.Op123.tgz.enc.sig
4. SqlGuard-11.Op125.tgz.enc.sig

Please choose the patches to remove by item number (1 to 4)
Specify multiple patches with comma separated numbers
Specify ALL for all
q to quit

Patch item number(s): all
SqlGuard-11.Op118.tgz.enc.sig removed
SqlGuard-11.Op121.tgz.enc.sig removed
SqlGuard-11.Op123.tgz.enc.sig removed
SqlGuard-11.Op125.tgz.enc.sig removed
Ok
```

store system patch preservation [on | off]

When patch preservation is turned *on*, Guardium patches are not automatically deleted after an installation failure. You can attempt reinstallation after fixing issues, if any.

Store system patch install

Installs a single patch or multiple patches as a background process. The *ftp* and *scp* options copy a compressed patch file from a network location to the IBM Guardium appliance. A compressed patch file can contain multiple patches, but you can install only one patch at a time. To install more than one patch, choose all the patches that need to be installed, separated by commas. Internally the CLI submits requests for each patch on the list (in the order that is specified by the user). The first patch takes the request time that is provided by the user and each subsequent patch runs 3 minutes after the previous one. In addition, CLI checks to see whether any specified patches are already requested and does not allow duplicate requests.

Use the *sys* option when you install a second (or subsequent) patch from a compressed file that was copied to the IBM Guardium appliance by previously using this command.

To display a complete list of applied patches, see the Installed Patches report from the Guardium UI. Find this report from Manage > Reports > Install Management > Installed Patches, Manage > Maintenance > General > Installed Patches, or Reports > Guardium Operational Reports > Installed Patches.

In the **store system patch install** CLI command, you can choose multiple patches from the list.

Syntax

store system patch install <type> <date> <time>

type - The installation type - **cd** | **ftp** | **scp** | **sys**

date, time - The patch installation request time, date is formatted as *YYYY-mm-dd*, and time is formatted as *hh:mm:ss*

If no date and time are provided, or if you enter NOW, the installation request time is NOW.

Parameters

Regardless of the option selected, you are prompted to select a patch to apply, for example:

Please choose one patch to apply (1-n,q to quit):

cd - - To install a patch from a CD, insert the CD into the IBM Guardium CD ROM drive before you run this command. A list of patches that are contained on the CD are displayed.

ftp or scp -- To install a patch from a compressed patch file located somewhere on the network, use the *ftp* or *scp* option, and respond to the prompts shown. Be sure to supply the full path name for the patch, including the file name. For example:

```
Host to import patch from:  
User on hostname:  
Full path to the patch, including name:  
Password:
```

For **store system patch install scp**, you can use a wildcard (*) for the patch file name.

The compressed patch file is copied to the Guardium appliance, and a list of patches contained on file displays.

sys - Use this option to apply a second or subsequent patch from a patch file that has been copied to the IBM Guardium appliance by a previous store system patch execution.

The store system patch install command does not delete the patch file from the IBM Guardium appliance after the installation. While you need not remove the patch file, as same patches can be reinstalled over existing patches and keeping patch files around can aid in analyze various problems, a user may remove patch files by hand or use the CLI command diag (Note, the CLI command diag is restricted to certain users and roles.)

To delete a patch install request, use the CLI command **delete scheduled-patch**.

Show command

```
show system patch <available | installed | preservation | staged | status >
```

Where:

- **available** - Displays the patches that are available for installation.
- **installed** - Displays the patches that are being installed or already installed.
- **preservation** - Displays the patch preservation status. When preservation is turned *off*, a patch is deleted after a failed installation attempt. When preservation is turned *on*, the patch is not deleted and you can attempt installation again.
- **staged** - Displays the patch files that are residing in the patches directory.
- **status** - Displays the status of a patch that is currently being installed.

store system public key

This command shows the outbound public SSH key for the standard users. The outbound SSH key pair is generated internally by the appliance, rather than stored from user input. If you adopt the public SSH key generated by the appliance, you can set up SSH export for the standard users: cli, grdapi, and tomcat All of the standard users use a common outbound SSH key.

12.0 Syntax

```
store system public key <cli | grdapi| tomcat | reset>
```

```
store system signature [on | off]
```

Where:

- **cli, grdapi, or tomcat** - Stores an existing public SSH key in the respective path.
- **reset** - Regenerates the outbound SSH Keys for the standard users.
Where --yes causes the command to reset automatically.

Show command

Displays an existing system public key for the CLI, GuardAPI, or Tomcat. If the public key does not yet exist, use **show system public key** to generate new outbound SSH keys. The SSH key pair is associated with the standard users: cli, grdapi, tomcat, and root.

```
show system public key < cli | grdapi | tomcat >
```

store system public key authorized

This command allows users to connect to the Guardium appliance by using SSH keys instead of passwords.

Syntax

```
store system public key authorized
```

Create the public key either with the **ssh-keygen** command or with the **show system public key** CLI command.

Note: How you create and store a public key with the **ssh-keygen** command depends on your operating system. For more information, see documentation for using **ssh-keygen** for your operating system.

Show command

Display the contents of an existing authorized public key.

```
show system public key authorized
```

Note: You can use the **ssh-keygen** command to create a public key. The exact commands depend on your operating system and other factors. Guardium suggests that you use the default location when you create the key.

After you create the key, store and use it as follows:

1. Connect to the Guardium appliance as the **cli** user:

```
ssh cli@guardium_host
```

2. Add the newly created public key:

```
store system public key authorized
```

3. At the prompt, paste the contents of the public key:

```
Please paste the SSH public key content here. Then press <ENTER> to continue.
```

The following message displays if the key is added:

```
Key for your_email@example.com is added  
ok
```

4. Run the following command to make sure that the key is available.

```
show system public key authorized  
your_email@example.com  
ok
```

5. You can now connect to the Guardium appliance that uses public key authentication. For example:

```
ssh cli@guardium_host
```

Note: If you specify a file name (rather than using the default id_rsa), then use the -i option when you run the **ssh** command and specify the location of the private key. For example,

```
ssh -i ~/.ssh/different_key_name cli@guardium_host  
IBM Guardium, Command Line Interface (CLI)
```

Delete command

delete system public key authorized

Displays a list of available public keys. Specify the number of the key that you want to delete.

store system public-transfer-key

Creates, deletes, and regenerates the transfer ssh-key pair for transferring data to a remote host by using the ssh-key pairs. For more information, see [Enabling ssh-key pairs for data archive, data export, data mart](#).

Syntax

```
store system public-transfer-key <create | delete | regenerate >
```

Where:

create - Create the ssh-key pair.

delete - Delete the ssh-key pair.

regenerate - Delete the existing ssh-key pair and then creates a new ssh-key pair.

Show command

```
show system public-transfer-key
```

store system remote-root-login

Enable/disable SSH (root access). Secure Shell or SSH is a network protocol that allows data to be exchanged by using a secure channel between two networked devices.

Syntax

```
store system remote-root-login ON|OFF
```

Show command

```
show system remote-root-login
```

Returns the public part of the transfer key.

store system ssh

This command sets the security options on the ssh service for the system.

Syntax

```
store system ssh <secure|default>
```

Where:

- **secure** - Improves the SSH key exchange algorithm (KEX).
- **default** - Turns secure KEX off.

After you run this CLI, the SSH service restarts.

store system scp-ssh-key-mode

Enable/disable the scp-ssh-key-mode, for enabling ssh-key pairs for data archive, data export, and data mart, without passwords. For more information, see [Enabling ssh-key pairs for data archive, data export, data mart](#).

store system scp-ssh-key-mode on|off

Show command

show system scp-ssh-key-mode

store system serialtty

In some environments, the serial TTY is not available so it cannot ever be started successfully. Potentially, this can appear in the system log and be forwarded to SIEM. This is enabled by default to permit connectivity, but can be disabled later if it is determined that serial consoles are unavailable to the system.

Syntax

store system serialtty <on, off>

Show command

show system serialtty

Reports whether or not serial TTYs are enabled on the system.

Reports either:

Serial TTY consoles are enabled on this system.

Serial TTY consoles are disabled on this system.

store system scheduler

Scheduling is managed by a timing mechanism within the IBM Guardium application. If the timing function is disrupted, it will restart after the restart interval designated by this CLI command.

Use store system scheduler restart_interval [5 to 1440 or -1] to restart the timing function after 5 minutes to 1440 minutes. The default is -1, which means the timing restart mechanism is not installed.

Use store system scheduler wait_for_shutdown [ON | OFF] to restart the scheduler after all jobs currently running finish. The parameters are ON or OFF.

Syntax

store system scheduler restart_interval [5 to 1440 or -1]

store system scheduler wait_for_shutdown [ON | OFF]

Show command

show system scheduler

store system service_status

Use this CLI command to enable or disable certain Guardium appliance services.

Syntax

store system service_status [enable | disable] <service-name>

Where,

- enable, disable - Specify whether to enable or disable a specified service.
- *service-name* - The name of a Guardium service that you can start or stop.

Run **store system service_status** with *enable* or *disable* to see the list of services that you can change.

Show command

Syntax

show system service_status [all | <service-name>]

Display the status of all available Guardium appliance services or specify a service to view. Run **show system service_status** with no parameters to see the list of services that you can view.

store system shared secret

Sets the system's shared secret value to the specified value. This key must be the same for a Central Manager and all appliances it manages; or an Aggregator, and all appliances from which it aggregates data. After an appliance has registered for management by a Central Manager, the shared secret on that unit is no longer used. (You cannot unregister a unit from Central Management by changing this value.)

Dynamic password for aggregator OS user

The aggregator password is the <the current password> concatenated with the shared secret, meaning: password=<current passwd><share secret>

Users need to make sure the collectors' shared secret and the aggregator's shared secret is the same, otherwise the SCP transfer fails from the collector to the aggregator (This is a requirement for managed units and aggregators, collectors and aggregators, and export setup screen). The shared secret can be set both from CLI and from the System pane in the Admin Console tab.

Syntax

store system shared secret <key>

store system signature [on | off]

This command is deprecated in Guardium version 12.1.

When turned *off*, enables deployment of apps that do not have signatures. Turn *off* store system signature when you are testing an app on your Guardium system; otherwise the app is blocked. In production this parameter should be *on* since you are using certified apps from the App Exchange.

Syntax

store system signature [on | off]

store openssl_sha1_signature

12.1 and later Use this CLI command to enable or disable sha-1. Turn sha-1 *on* to upload the GIM bundles. After you upload the bundles, you can turn sha-1 *off*.

Syntax

store openssl_sha1_signature [on|off]

Show command

show openssl_sha1_signature

store system snif-alerts-facility

This parameter allows the user to configure the facility for snif generated alerts. Previously alerts directly generated by snif used the user facility while indirect alerts used the daemon facility (via the guard_sender utility).

Syntax

store system snif-alerts-facility <facility>

USAGE: store snif-alerts-facility <facility>

facility is one of: **daemon ftp local0 local1 local2 local3 local4 local5 local6 local7 lpr user**

The default facility is daemon.

Show command

show system snif-alerts-facility

store system snif-buffers-reclaim

Use this CLI command only when directed by IBM Guardium Technical Services.

The new configuration takes effect after you run the **restart inspection-core** CLI command.

Syntax

store system snif-buffers-reclaim [ON | OFF]

Show command

show system snif-buffers-reclaim

store system snif-thread-number

Use this CLI command to specify how many threads are running.

The new configuration takes effect after you run the **restart inspection-core** CLI command.

Syntax

store system snif-thread-number [new | default]

Show command

show system snif-thread-number

Snif is running with 6 threads on the 32-bit system.

show system snmp engineid

Use this CLI command to display the SNMP engine ID for the IBM Guardium appliance.

Syntax

show system snmp engineid

store system snmp contact

Stores the email address for the SNMP contact (syscontact) for the IBM Guardium appliance. The default is `info@guardium.com`.

Syntax

store system snmp contact <email-address>

Show command

show system snmp contact

store system snmp location

Stores the SNMP system location (syslocation) for the IBM Guardium appliance. The default is `Unknown`.

Syntax

store system snmp location <string>

Show command

show system snmp location

store system snmp query community

Stores the SNMP system query community for the IBM Guardium appliance. The default is `guardiumsnmp`. This command is valid only for SNMP version 2c.

Syntax

store system snmp query community <string>

Show command

show system snmp query community

store system snmp update_user

Use this command to update an existing SNMP user account for an SNMP version 3 system.

Syntax

store system snmp update_user

This command overwrites all the information for an existing SNMP user account. Similar to `store system snmp user create`, you need to provide a username, authentication protocol and passphrase, and encryption protocol and passphrase.

store system snmp user

Use this command to create or remove an SNMP user account for an SNMP version 3 system. You can create only one SNMP user account. The default encryption protocol is AES-128.

Syntax

store system snmp user [create | delete]

Where:

- `create` - Creates an SNMP user account for this machine. To create an SNMP user account, you need to provide a username, authentication protocol and passphrase. The CLI walks you through the process. For example,

```
> store system snmp user create
Enter SNMPv3 user name:
fred
Enter authentication protocol < MD5 | SHA > or 'q' to quit. (Default authentication protocol is MD5) :
md5
Create authentication passphrase (8 to 12 chars): *****
Re-enter authentication passphrase: *****
Enter Encryption protocol < DES | AES > or 'q' to quit. (Default encryption protocol is AES.):
des
Create encryption passphrase (8 to 20 chars): *****
Re-enter encryption passphrase: *****
ok
```

After you provide the required information, Guardium adds the SNMP user. For example:

```
adding the following line to /var/lib/net-snmp/snmpd.conf:
    createUser fred MD5 "fred1234" DES 1234fred
adding the following line to /etc/snmp/snmpd.conf:
    rouser fred
ok
```

- `delete` - Removes the current SNMP user account.

Show command

```
show system snmp user
```

store system snmp version

Use this CLI command to switch between SNMP version 2c and SNMP version 3. The default is v2c. If your system uses SNMPv3, use this command to update Guardium.

Syntax

```
store system snmp version [v2c | v3]
```

Where:

- v2c: SNMP version 2c
- v3: SNMP version 3

Show command

```
show system snmp version
```

Examples

```
test.usma.ibm.com> show system snmp version
SNMP Version : v2c
ok
test.ibm.com> store system snmp version v3
snmp version v3 enabled
ok
test.usma.ibm.com> show system snmp version
SNMP Version: v3
ok
```

store system ssh-dsa state

This command enables or disables SSH DSA authentication.

Syntax

```
store system ssh-dsa state [ON | OFF ]
```

Where:

- ON: Activates the DSA host keys that are propagated from an upgrade. If no such keys exist, then DSA host keys are generated on SSH start-up.
- OFF: Inactivates any DSA host keys. DSA is inactivated on SSH start-up.

Show command

```
show system ssh-dsa state
```

store system sshd-max-connection

This command allows the maximum number of concurrent sshd connections to be configured. The range is between 100-500. The default value is 250.

Note: This command stops existing connections and restarts the ssh daemon on the Guardium appliance.

12.0 Syntax

```
store system sshd-max-connection <value>
```

12.1 and later Syntax.

Where --yes causes the command to run automatically.

Show command

```
show sys sshd-max-connection
```

store system time_server

Sets the hostname of up to three time (Network Time Protocol, or NTP) servers. To enable the use of a time server, set the **store system time_server state** command to *on*. To define one or more time servers, use the **store system time_server hostnames** command.

Note: Guardium does not support hostnames for a time server when the underlying IP address for that hostname is dynamic. The hostname must resolve to a static IP address. If you change the IP address, restart the network to sync to the new time server IP address.

Syntax

```
store system time_server [ hostnames | state ]
```

Where:

- **hostnames** - Enter up to three time server IP addresses or hostnames. Click Enter to stop entering hostnames.
- **state <on | off>** - Toggle the time server *on* or *off*.

Delete command

```
delete time_server
```

Show command

```
show system time_server <all | diagnostics | hostnames | state>
```

Where:

- **all** - Displays the name or IP address of any chrony time servers along with their current status.
- **diagnostics** - Runs the time server daemon (chronyd) and sends the output directly to the screen. For example:

```
CLI> show system time_server diagnostics
Output from chronyc sources :
MS Name/IP address      Stratum Poll Reach LastRx Last sample
=====
^- 168.22.22.74          3   10   377   711   -1448us[-1472us] +/-   66ms
^- circle.ellipse.net     2   10   377   681   -976us[-1000us] +/-   45ms
^- h134-222-111-62.sample.b> 2   10   175   78m   -2451us[-3049us] +/-   33ms
^* time.example.com       3   10   377   542   -300us[-324us] +/-   11ms
^- ns01.abc.example.com   4   10   377   737   -3167us[-3191us] +/-   34ms
ok
```

- **hostnames** - Shows the names or IP addresses of currently active time servers.
- **state** - Displays the status of the chrony time service.

store system websmartcard

The command enables or disables smart card authentication. For more information, see [Enabling Smart card authentication](#).

Syntax

```
store system websmartcard [on | off]
```

Show command

```
show system websmartcard
```

store system admin-only

When smart card or SAML authentication is enabled, run the **store system admin-only on** command to allow the *admin* or *accessmgr* accounts to log in to the Guardium system by using a standard login and password screen.

When enabled, the *admin* or *accessmgr* access a separate login page by appending /admin to the URL of the Guardium system. Example URL: *https://www.[your_guardium_system's_domain_name].com:[port_number]/admin*.

For more information, see [Enabling Smart card authentication](#)

Syntax

```
store system admin-only [on | off]
```

Note: This command restarts the GUI.

Show command

```
show system admin-only
```

User account, password, and authentication CLI Commands

Use these CLI commands to configure user accounts, passwords, and authentication.

Authenticating GuardAPI commands with set guiuser

Before you can call any GuardAPI commands, you must log in to the command line interface (CLI) with one of the default CLI accounts (guardcli1, guardcli2...guardcli9), and then run the **set guiuser** CLI command. This authentication is required to prevent users with limited roles in the GUI from gaining unauthorized access to GuardAPI commands. For more information about the GuardAPI commands, see [Using GuardAPI commands](#).

Certain GuardAPI commands are available only for certain user roles. For example, you must set the *guiuser* role to *accessmgr* and *cli* to view or use the [create_user](#), [set_user_roles](#), or [update_user](#) GuardAPI commands. Create a user and password with appropriate roles from the *accessmgr*. For more information, see [Creating a user who can run GuardAPI commands](#).

set guiuser

To use the *guardcli* accounts with GuardAPI commands, you must use **set guiuser** to associate the *guardcli* account to the local user and password.

Note: If LDAP authentication is used, enter the LDAP user and LDAP password as the local user and password.

Syntax

```
set guiuser <gui_user or LDAP user> password <password or LDAP password>
```

Example

You must run **set guiuser** whenever you want to use GuardAPI commands. When you set the *guiuser* for the first time, you are prompted to change the password, as shown in the following example.

```
$ ssh guardcli2@mycorp.com
IBM
Guardium , Command Line Interface (CLI)
```

```
guardcli1@al.corp.com's password:  
Last login: Thu Nov  4 14:56:34 2020 from 123.al.corp.com  
123.al.corp.com> set guiuser Hadrian.Swall  
Enter current password:  
First login as Hadrian.Swall. Please change the default password.  
Enter new password:  
Re-enter new password:  
ok
```

Note: When you change the password, you cannot reuse the last 10 passwords.

Show command

```
show guiuser
```

Password Control Commands

Use the following commands to control user passwords, as follows:

- [store password disable](#): Sets the number of days after which an inactive account is disabled.
- [store password expiration](#): Sets the number of days after which a password expires.
- [store password validation](#): Enables or disables the hardened password validation rules.

Account Lockout Commands

Use the account lockout commands to disable a Guardium user account after one or more failed login attempts. Use these commands to:

- Enable or disable the feature. See [store account lockout](#).
- Set the maximum number of login failures allowed an account within the specified number of seconds. See [store account strike count](#) and [store account strike interval](#).
- Set the maximum number of failures allowed an account for the life of the Guardium appliance. See [store account strike max](#).
- To unlock the admin user account if it becomes locked, see [unlock admin](#).

After a Guardium user account is disabled, users with the accessmgr role, or the admin user, can enable the account from the Guardium portal.

Example

The following example locks out an account, locks an account after five login failures within 60 seconds, and sets the maximum number of failures that are allowed to 999.

```
store account lockout on  
store account strike count 5  
store account strike interval 60  
store account strike max 999
```

Note:

If the admin user account is locked, use the [unlock admin](#) command to unlock it.

If account lockout is enabled, setting the strike count or strike max to zero does not disable that type of check. On the contrary, it means that after just one failure the user account is disabled!

store account lockout

Enables (on) or disables (off) the automatic account lockout feature, which disables a user account after a specified number of login failures.

Syntax

```
store account lockout <on | off>
```

Show command

```
show account lockout
```

store account strike count

Sets the number of failed login attempts (n) in the configured strike interval before the account is disabled.

Syntax

```
store account strike count <n>
```

Show command

```
show account strike count
```

store account strike interval

Sets the number of seconds (n) during which the configured number of failed login attempts must occur to disable the account.

Syntax

```
store account strike interval <n>
```

Show command

```
show account strike interval
```

store account strike max

Sets the maximum number (n) of failed login attempts to be allowed for an account over the life of the server before the account is disabled.

Syntax

store account strike max <n>

Show command

show account strike max

store disable_sha1_passwords

By default, the Guardium GUI user passwords are hashed with a strong password hashing algorithm. The **store disable_sha1_passwords** CLI command allows admins to remove existing passwords that are weakly hashed from their Guardium appliances.

Note: In an upgrade scenario, this command removes only weak passwords for users who have logged in since the upgrade.

Syntax

store disable_sha1_passwords [true | false]

Run the **store disable_sha1_passwords true** command on the central manager and all backup central managers, if applicable.

Example:

```
>store disable_sha1_passwords true
> User passwords will now be hashed with a strong password hashing algorithm.

>store disable_sha1_passwords false
> User passwords will now be hashed with a weak password hashing algorithm.
Weak password hashing algorithms may violate your company compliance requirements.
```

Show command

show disable_sha1_passwords

The show command returns the current settings for password hashing.

Example:

```
>show disable_sha1_passwords
>SHA1 passwords are allowed.
```

Note: In an upgrade scenario, the show command returns the users who have not logged in since the upgrade.

store guarduser_state

From the cli account for your Guardium appliance, you can now enable or disable the guardcliN (that is guardcli1 to guardcli9) login IDs. You can only change or show the status of one ID at a time.

Syntax

store guarduser_state <disable|enable> <guardcli1..guardcli9>

For example, to disable guardcli4:

store guarduser_state disable guardcli4

Show command

show guarduser_state guardcli4

store password disable

Sets the number of days of inactivity after which user accounts are disabled. When set to 0 (zero), no accounts are disabled by inactivity. At installation, the default value is zero. You must restart the GUI after you change this setting (see **restart gui**).

Syntax

store password disable <days>

Show command

show password disable

store password expiration

Sets the number of days until a user's password expires. The default value is 60 for *cli* and *guardcli1 - guardcli9* users, and 90 for *gui* users. The minimum is 1 for *cli* and *guardcli1 - guardcli9* and 0 for *gui*.

Syntax

store password expiration [cli | guardcli1 - guardcli9 | gui] <days>

Where:

- - *cli*: The CLI user.
 - *guardcli1* through *guardcli9*: One of the guardcli users.
 - *gui*: The GUI user. If you change the GUI password expiration, you must restart the GUI.
- <days>: The number of days before the password expires.
 - The maximum number of days for *cli* and *guardcli* users is 60.
 - For *gui* users only, you can disable the password expiration in practice by setting the expiration days to a very high number (up to 7300 days, or 20 years).

The account user is prompted to reset the password the first time they log in after the current password expires.

Show command

show password expiration

store password requirements

If **store strong_password_enable** is enabled, then you can specify certain password requirements for *cli* and *guardcli* accounts to meet your corporate standards.

Syntax

store password requirements <parameter> <number>

Where *parameter* is one of the parameters in the following table, and *number* is the requirement for that parameter.

Table 1. Parameters for store password requirements CLI

| Parameter | Meaning |
|-----------------|---|
| max_repeats | Specify the maximum number of characters of a single type (that is: digits, upper case letters, lower case letters, or symbols) that can be consecutively repeated in a password. |
| minimum_length | Specify the minimum password length. |
| minimum_digits | Specify the minimum required number of digits (0 - 9). |
| minimum_lower | Specify the minimum required number of lower case letters (a - z). |
| minimum_upper | Specify the minimum required number of upper case letters (A - Z). |
| minimum_symbols | Specify the minimum required number of special characters (from Table 2). |

Example

```
>store password requirements max_repeats 2  
>store password requirements minimum_digits 2
```

Show command

show password requirements

Sample output

```
> show password requirements  
Passwords must conform to the following rules:  
    cannot be a dictionary word  
    maximum repeated characters: 2  
    maximum repeated characters within a class: 4  
    minimum digits: 2  
    minimum length: 15  
    minimum lower case: 3  
    minimum symbols: 1  
    minimum upper case: 3  
    At least one each of digits, uppercase, lowercase, symbols.
```

store password validation

Turns password validation on or off. The default value is on. Running this command restarts the GUI to apply this setting.

When password validation is enabled, passwords must be eight or more characters long, and must include at least one of each:

- An uppercase letter (A-Z)
- A lowercase letter (a-z)
- A number (0-9)
- A special character from [Table 2](#)

When password validation is disabled (not recommended), any length or combination of characters is allowed.

Syntax

store password validation <on | off>

Show command

show password validation

Table 2. Special characters for
Guardium passwords

| Character | Description |
|-----------|-------------|
| @ | At sign |
| # | Number sign |

| Character | Description |
|-----------|---------------------------|
| \$ | Dollar sign |
| % | Percent sign |
| ^ | Circumflex accent (carat) |
| & | Ampersand |
| . | Full stop (Period) |
| ; | Semicolon |
| ! | Exclamation mark |
| - | Hyphen (minus) |
| + | Plus sign |
| = | Equals sign |
| _ | Underscore |

store strong_password_enable

Use this command to enable or disable strong password checking. This setting applies only to local passwords and does not affect passwords that are validated against external directories such as LDAP. Restart the Guardium GUI for the changes to take effect.

Strong passwords must be at least 15 characters and follow the rules that are described in [store_password_validation](#).

If strong passwords are enabled, you can use [store_password_requirements](#) to specify your own password validation rules.

In addition, when **strong_password_enable** is on, Guardium ensures that the GUI password is not expired, based on the value of the [store_password_expiration](#) command.

Syntax

```
store strong_password_enable [on|off]
```

Show command

```
show strong_password_enable
```

store user password

Use this command to reset the CLI user password. To simplify the support process, Guardium suggests that you keep the CLI user password assigned initially by Guardium. You cannot retrieve the CLI user password after it is set. If you lose this password, contact Guardium Support to have it reset.

Syntax

```
store user password
```

You are prompted to enter the current password, and then the new password (twice). The password values that you enter on the keyboard do not display on the screen.

The CLI user password requirements differ from the requirements for user passwords. The CLI user password must be at least 8 characters long, and must contain at least one each of the following types of characters:

- Lowercase letters
- Uppercase letters
- Special characters from [Table 2](#).

Running this CLI command also updates the change-time record in the password expiration file.

unlock accessmgr

Use this command to enable the Guardium accessmgr user account after it is disabled. This command does not reset the accessmgr user account password.

Note: Only users with admin role are allowed to run this CLI command.

Syntax

```
unlock accessmgr
```

```
restart gui
```

unlock admin

Use this command to enable the Guardium admin user account after it is disabled. This command does not reset the admin user account password.

Note: Only users with admin role are allowed to run this CLI command.

Syntax

```
unlock admin
```

```
restart gui
```

Authentication commands

The following commands display or control the type of authentication used.

store auth

Use this command to reset the type of authentication that is used for login to the Guardium appliance, to SQL_GUARD (that is, the local Guardium authentication, the default).

Syntax

store auth SQL_GUARD

Show command

show auth

store cli_userauth

CLI users can be authenticated locally or by LDAP, but not both.

To enable LDAP authentication for CLI users, including GUARDCLI accounts, use the following command:

Syntax

store cli_userauth ldap --server <server> --basedn<basedn> --rdntype<rdntype> [port number] [usetls]

Note: The default TLS port number is 636 and the default plain is 389.

Example:

```
store cli_userauth ldap --server ldapserver.example.com --basedn ou=people,dc=guardium,dc=example,dc=com --rdntype uid
Validating server and port:
OK
Configuring LDAP authentication with
Server: 'ldapserver.example.com'
Port: '389'
Basedn: 'ou=people,dc=guardium,dc=example,dc=com'
RDN Type: 'uid'
Use TLS: '0'
Please confirm [y/n] y
Authentication is set to LDAP
OK
```

Note: Trusted certificates that are required for LDAP with SSL option must be imported from the GUI.

When LDAP authentication is enabled, the following commands are not available:

1. **show password expiration cli**
2. **store password expiration cli**
3. **store user password**

The following message is displayed when you run these commands:

CLI user authentication is managed externally. Please contact your system administrators.

To disable LDAP authentication for CLI users, including GUARDCLI accounts, use the following command:

Syntax

store cli_userauth default

Show command

show cli_userauth [details]

Related reference

- [create_user](#)
- [list_user_roles](#)
- [set_user_roles](#)
- [update_user](#)

GuardAPI and REST API commands

GuardAPI commands provide access to Guardium® functionality from the command line. Many GuardAPI commands also have REST API equivalents.

REST API commands are described along with the GuardAPI commands. Use the [Guardium API A-Z Reference](#) to find information about individual GuardAPI and REST API commands.

- [**Using GuardAPI commands**](#)
Learn how to use the GuardAPI commands.
- [**Using Guardium REST APIs**](#)
Use the Guardium REST API to include many Guardium API commands in your applications or anywhere that a REST API is useful.
- [**Guardium API A-Z Reference**](#)
All of the Guardium GuardAPI commands, arranged alphabetically. Click the GuardAPI command for more information about that command. If the GuardAPI command has a REST API interface, the REST call is also provided.
- [**Access management APIs**](#)
Use these commands to manage access to the Guardium system. Many of these commands require the accessmgr role.

- [**Active threat analytics and risk spotter APIs**](#)
Use these commands to configure Active threat analytics and Risk spotter.
- [**Alerter APIs**](#)
Use these APIs to manage alerter functions.
- [**Archive, export, import, purge, and restore APIs**](#)
Use these functions to configure archive, restore, purge, export, and import, of results and data.
- [**Assessment APIs**](#)
Use these APIs to add, delete, and update Vulnerability Assessment (VA) functions.
- [**Auto-discovery APIs**](#)
Use these GrdAPI commands to create, modify, list and run the Auto-discovery processes.
- [**Big Data Intelligence APIs**](#)
Run these commands, on your central manager, to manage extraction of datamarts to the Big Data datasource (GBDI), and to pull big data into Guardium for monitoring, reports, and so on.
- [**Catalog entry APIs**](#)
Use these commands to manage catalog entries. Catalogs are used to track data archive files and result archive files that were created on the servers.
- [**Central management APIs**](#)
Use these APIs to view and set load balancing parameters, view the current load map, manage S-TAP® and managed unit group associations, and manage backup central managers.
- [**Classification APIs**](#)
Use the following GuardAPI commands for Classification policy configuration, for test automation and, for scripting of prerequisite data preparation.
- [**Cloud datasource APIs**](#)
Use these commands to define, manage, update, and delete cloud datasources.
- [**Configuration Auditing System \(CAS\) APIs**](#)
Use these commands to configure and manage Configuration Auditing System (CAS) hosts, templates, and template sets.
- [**Data mart APIs**](#)
Use these commands to manage your data marts.
- [**Database user APIs**](#)
Use these commands to maintain database user mapping, non-credential scans and manage debug levels.
- [**Datasource APIs**](#)
Use these commands to create, list, delete, and update datasource and datasource references.
- [**Datasource credential management APIs**](#)
Use these commands to manage datasource credentials.
- [**Entitlement optimization APIs**](#)
Use these API commands to enable and configure the Entitlement optimization datasources and reporting.
- [**External feed APIs**](#)
Use these commands to create mappings for external feeds.
- [**File Activity Monitor APIs**](#)
Use the following GuardAPI commands to enable and disable the file activity monitor, configure the file Investigation Dashboard activity and entitlement extractions schedule, and get information on the file activity monitor.
- [**Guardium Insights APIs**](#)
Use these APIs to manage the connection between Guardium Data Protection and Guardium Insights.
- [**Guardium Installation Manager \(GIM\) APIs**](#)
Use these APIs to assign, cancel, list, remove, and update Guardium Installation Manager (GIM) functions.
- [**Guardium universal connector APIs**](#)
Use these functions to start, stop, and check the status of the Guardium universal connector, and to modify the MongoDB filters.
- [**Group APIs**](#)
Use these commands to create, list, and delete groups, hierarchical groups, and group members and manage aliases for groups.
- [**Health analyzer APIs**](#)
Use these commands to configure the disk and database health analyzer.
- [**Hadoop monitoring APIs**](#)
Use these APIs to add, update, delete, and view the clusters and services on the clusters for all types monitoring on Hadoop.
- [**Investigation dashboard APIs**](#)
Use these APIs to enable, disable, or configure the investigation dashboard (quick search) features and parameters.
- [**Miscellaneous APIs**](#)
Use these commands for various tasks that do not fall into other categories.
- [**Native audit APIs**](#)
Use these commands to enable or disable DB Audit (native audit) on a cloud database, add and remove objects from the Object Audit (audit trail), and get configuration, collectors, and objects details.
- [**Outliers detection APIs**](#)
Use these API commands to enable, disable, and configure the Outliers Detection function.
- [**Policy and rule APIs**](#)
Use these commands to manage policies and policy rules.
- [**Process Control APIs**](#)
Use these commands to manage various process control functions.
- [**Query rewrite APIs**](#)
Use these commands to automate testing or create definitions for certain complex queries that cannot be done from the user interface.
- [**Reports and report generation APIs**](#)
Use report generation APIs to manage reports and distributed reports, and to take the output from one Guardium report or entity and feed it as the input for another Guardium entity.
- [**Schedule and job dependencies APIs**](#)
Use these APIs to set schedules for and dependencies between jobs.
- [**Solr APIs**](#)
Run these commands on your central manager and managed units to manage their (internal Guardium) Solr database.
- [**S-TAP and inspection engine APIs**](#)
Use these commands to manage your S-TAPs and their inspection engines.
- [**S-TAP for IBM i APIs**](#)
Use these commands to create, list, delete, restart, and set i-S-TAP functions.
- [**Threat detection analytics APIs**](#)
Use these GuardAPI commands to configure threat detection analytics.

Using GuardAPI commands

Learn how to use the GuardAPI commands.

Accessing GuardAPI commands

GuardAPI is a set of commands that you can use to automate repetitive tasks, which is especially valuable in larger implementations. Use the GuardAPI functions to quickly perform operations such as creating datasources, maintaining user hierarchies, or maintaining Guardium® features such as S-TAP®, just to name a few. For a list of the available GuardAPI commands, see [Guardium API A-Z Reference](#).

Before you can use GuardAPI commands, you need a local user and password (or an LDAP username) with appropriate roles and permissions. The GuardAPI commands that are available to you depend on your roles. For more information, see [Creating a user who can run GuardAPI commands](#).

To access GuardAPI commands:

1. From the CLI, log in as one of the guardcli users (that is, guardcli1 to guardcli9). For example:

```
ssh guardcli2@company.com
```

2. Run the **set guiuser** CLI command to associate the new user with the guardcli user. The first time you log in, you must change your password (except for LDAP users). For example:

```
company.com> set guiuser Hadrian.Swall
Enter current password:
First login as Hadrian.Swall. Please change the default password.
Enter new password:
Re-enter new password:
ok
```

Note: When you change the password, you cannot reuse the last 10 passwords.

For more information about **set guiuser**, see [Authenticating GuardAPI commands with set guiuser](#).

3. If your system has multi-factor authentication enabled, Guardium will request that you provide secondary authentication. Select the notification type by its number. For example:

```
mycompany.com> set guiuser Hadrian
Enter current password:
Secondary authentication is required for Hadrian
Please select a notification method:
0: cell phone (XXX-XXX-8846) : auto
1: cell phone (XXX-XXX-8846) : push
2: cell phone (XXX-XXX-8846) : sms
3: cell phone (XXX-XXX-8846) : phone
Q/q: Quit

2
Enter SMS passcode:
ok
```

Note: The available notification methods depend on how multi-factor authentication is configured for your site.

4. In this case, the user, Hadrian Swall, can now use any GuardAPI commands that are available for the associated roles.

Finding GuardAPI command information

GuardAPI is a subset of CLI commands, all of which begin with the keyword **grdapi**.

- To list all GuardAPI commands available for your role, enter **grdapi** or **grdapi commands** with no arguments. For example:

```
> grdapi
or
> grdapi commands
```

You can also find information about all of the GuardAPI commands in the [Guardium API A-Z Reference](#).

- To display information for a particular command, enter the command followed by **--help=true**. For example:

```
CLI> grdapi list_entry_location --help=true
ID=0
function parameters :
fileName
hostName - required
path - required
ok
```

Note: For some parameters, the available options depend on factors such as your operating system, available databases, or licenses. In these cases, look for the complete parameter list for your system by running **--help=true** for that GuardAPI in the CLI.

- To display a values list for a parameter, enter the command followed by **--get_param_values=<parameter>**. For example:

```
CLI> grdapi create_group --get_param_values=appid
Value for parameter 'appid' of function 'create_group' must be one of:
Public
Audit Process Builder
Classifier
DB2 zOS Groups
Express Security
IMS zOS Groups
Policy Builder
```

```

Security Assessment Builder
ID=0
ok

• To search for GuardAPI commands given a search string use grdapi commands <search-string>. For example:

CLI> grdapi commands user
ID=0
Matching API Function list :
create_db_user_mapping
create_user_hierarchy
delete_allowed_db_by_user
delete_db_user_mapping
delete_user_hierarchy_by_entry_id
delete_user_hierarchy_by_user
execute_appUserTranslation
execute_ldap_user_import
list_allowed_db_by_user
list_db_user_mapping
list_user_hierarchy_by_parent_user
update_user_db

```

GuardAPI syntax

- Both the keyword and value components of parameters are case-sensitive.
- If a parameter value contains one or more spaces, it must be enclosed in double quotation marks, for example,

```
grdapi create_datasource type ="MS SQL SERVER" ...
```

- NULL values and empty strings: In general, when a value for a non-required parameter is not specified or is set to an empty string ("") GuardAPI converts the parameter to NULL when the function is called. That is, the parameter is ignored as if it were not specified.
If for example, you want to clear out a group from a policy rule, you might set that group to space (" ") and not an empty string (""). Using an empty string ("") signals that GuardAPI can ignore that group and not change that group selection.

For example,

```
grdapi update_rule fromPolicy=V8 ruleDesc="LogFull Details" dbUserGroup=" "
dbUser=" " objectGroup=" " commandsGroup=" "
```

Return Codes

The GuardAPI always returns a code in the first line of output, in one of the following formats:

Table 1. Return Codes

| Return Code | Description |
|----------------|---|
| ID=identifier | Success. The identifier is the ID of the object that is operated upon; for example, the ID of a group that was just defined. |
| ERR=error_code | Error. The error_code identifies the error, and one or more additional lines provide a text description of the error. See Table 2 for a list of common error codes. |

For example, if you use **create_group** to successfully define an objects group named *agroup*, the ID of that group is returned:

```

CLI> grdapi create_group desc=agroup type=objects appid=Public
ID=20001
ok
CLI>

```

You can then use that ID in the **list_group_by_id** command to display the group definition.

```

CLI> grdapi list_group_by_id id=20001
ID=20001
Group GroupId=20001
Group GroupTypeId=3
Group ApplicationId=0
Group GroupDescription=agroup
Group GroupSubtype=null
Group CategoryName=null
Group ClassificationName=null
Group Timestamp=2008-05-10 07:34:11.0
Group type = OBJECTS
Application Type = Public
Tuple Group
ok

```

If the GuardAPI fails, an error code is returned. For example, if you enter the **list_group_by_id** command again with an invalid ID, you receive the following message:

```

a1.corp.com> grdapi list_group_by_id id=20123
ERR=140
Could not retrieve Group - check Id.
ok

```

Common Error Codes

Error codes with a value less than 100 are for common error conditions. Error codes greater than 100 apply to specific functions.

For a complete list of GuardAPI error codes, enter **grdapi-errors** at the CLI command prompt.

Table 2. Common Error Codes

| Error | Description |
|-------|-------------|
|-------|-------------|

| Error | Description |
|-------|---|
| 0 | Missing parameters or unknown errors such as unexpected exceptions |
| 1 | An Exception has occurred, please contact Guardium support |
| 2 | Could not retrieve requested function - check function name. To list all functions call either the "grdap" or "grdap commands" with no arguments. To search by function name given a search string, use the "grdap commands <search-string>". |
| 3 | Too many arguments. To get the list of parameters for this function call the function --help=true |
| 4 | Missing required parameter. To get the list of parameters for this function call the function with --help=true |
| 5 | Could not decrypt parameter, check if encrypted with the correct shared secret |
| 6 | Wrong parameter format, specify a function name followed by a list of parameters using <name=value> format. |
| 7 | Wrong parameter value for parameter type |
| 8 | Wrong parameter name, please note, parameters are case-sensitive. |
| 9 | User has insufficient privileges for the requested API function |
| 10 | Parameter Encryption not enabled - shared secret not set. |
| 11 | Failed sending API call request to targetHost |
| 12 | Error Validating Parameter |
| 13 | Target host must be the ip address of the central manager |
| 14 | Target host is not managed by this manager. |
| 15 | Target host is not online |
| 16 | Target host cannot be specified on a standalone unit |
| 17 | User is not allowed to operate on the specified object |
| 18 | Target host cannot be specified |
| 19 | Missing end quote |
| 20 | User is not allowed to run grdap commands |
| 21 | --username and --source-host are grdap reserved words and cannot be passed on the command line. |
| 22 | A parameter name cannot be specified more than once, please check the command line for duplicate parameters. |
| 23 | Value not in constant list. |
| 24 | Not a valid encrypted value. |
| 25 | Not a valid parameter format - parameters should be specified as <name=value>, spaces are not allowed. |

GuardAPI Activity Log

The Guardium Activity Log records all GuardAPI commands that are executed on the system. To view the commands from the administrator portal, navigate to the User Activity Audit Trail report on the Guardium Monitor tab.

All GuardAPI activity is attributed to the cli user. Double-click the cli row in that report, and select the Detailed Guardium User Activity drill-down report. For each row, the report lists the following information:

- Every command entered.
- Any changes made.
- The IP address from which the command was issued.

Encrypted Parameters

GuardAPI is intended to be invoked by scripts, which may contain sensitive information, such as passwords for datasources. To ensure that sensitive information is kept encrypted at all times, the grdap command supports passing of one encrypted parameter to an API Function. This encryption is done using the System Shared Secret which is set by the administrator and can be shared by many systems, and between all units of a central management and/or aggregation cluster; enabling scripts with encrypted parameters to run on machines that have the same shared secret.

Note: Trying to run an API call with encrypted parameter on a system where shared secret was not set results in the following error message:

Parameter Encryption not enabled - shared secret not set

For Guard API scripts generated through the GUI, if encryption is required it is done using the shared secret of the system where script generation is performed.

The optional parameter encryptedParam is available on every grdap call. This parameter can be used to pass an encrypted value for another parameter.

The procedure for manual encryption is as follows:

1. Use the Parameter Encryption API.
The encrypt_value API accepts a value to encrypt and the target system's shared secret (key) and then prints out the encrypted value. If the key is not the system's shared secret it will print out a warning.

```
a1.corp.com> grdap encrypt_value --help=true
ID=0
function parameters :
key - required
valueToEncrypt - required
api_target_host
ok
```

Table 3. Encrypted Parameter

| Parameter | Description |
|-----------------|--|
| key | The target system's shared secret. |
| valueToEncrypt | The value to be encrypted. |
| api_target_host | In a central management configuration only, allows the user to specify a target host where the API will execute. On a Central Manager (CM) the value is the host name or IP of any managed units. On a managed unit it is the host name or IP of the CM. |

Example

```
a1.corp.com> grdapi encrypt_value valueToEncrypt="some value" key=guard
ID=0
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.7 (GNU/Linux)
jA0EA9gMCTEIJShudn0tgyTB9GL7wR79UL9X9DCaa6RkUQRbegG52o1A4gwOzmpHF
0qEhsd6Uz718rUsheUyX9v4=
=c1Cq
-----END PGP MESSAGE-----
```

2. Copy the generated content and embed within your CLI script.

```
example of cli.gsh code :
set guimuser johny_smith password 3we19s887s
  grdapi create_datasource type=oracle name=myOra host=somehost application=AuditTask owner=admin user=sa serviceName=ora
encryptedParam=password
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.7 (GNU/Linux)
jA0EA9gMCTEIJShudn0tgyTB9GL7wR79UL9X9DCaa6RkUQRbegG52o1A4gwOzmpHF
0qEhsd6Uz718rUsheUyX9v4=
=c1Cq
-----END PGP MESSAGE-----
```

3. Run the script to invoke GrdApi:

```
user> ssh cli@a1.corp.com user> ssh cli@a1.corp.com
```

Role validation for certain GuardAPI commands

Role validation implements controls on selected GuardAPI commands to consider the roles of the specific components (and not only the application) and disallow actions if the roles do not match.

For example, a user with the appropriate roles for Policy Builder can run the delete_rule API on any policy, regardless of the roles of this specific policy.

If you try to run an API for which you do not have the appropriate role or permissions, the CLI returns an error message.

Display attributes for certain users in Query-Report Builder

The admin user can see all query attributes in Query-Report Builder and non-admin users can see query attributes in Query-Report Builder, except those that are designed as admin only (IDs, for example).

There are some entities (such as FULL SQL) that have large numbers of attributes in them. By default, all attributes display for all users (admin and non-admin).

Two GuardAPI commands, **enable_special_attributes** and **disable_special_attributes** determine whether certain attributes display for certain users. For more information, see [enable_special_attributes](#) and [disable_special_attributes](#).

Note: When using GuardAPI in a central manager environment, be sure that you understand which components are defined on the central manager, and which components are defined on managed units. For information, see [Central Management](#).

Related concepts

- [Using Guardium REST APIs](#)

Related tasks

- [Working with API calls and reports](#)

Related reference

- [Guardium API A-Z Reference](#)

Using Guardium REST APIs

Use the Guardium® REST API to include many Guardium API commands in your applications or anywhere that a REST API is useful.

Guardium REST API overview

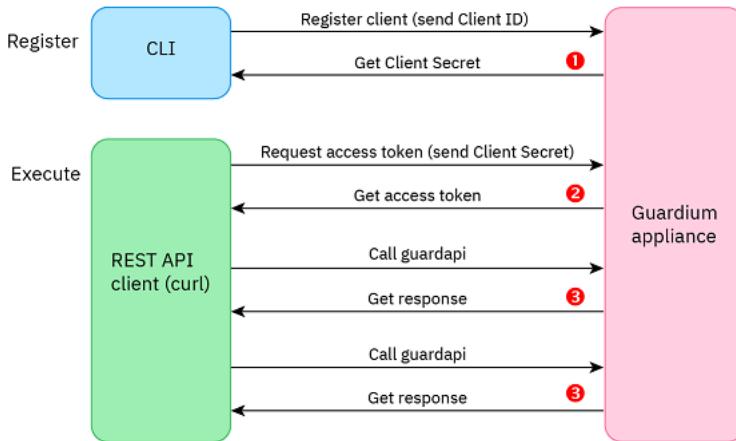
The Guardium REST API serves as a wrapper for the rich set of Guardium API (GuardAPI) command-line interface functions. After you register the REST API client on the Guardium collector, as described in [Calling REST APIs example](#), you can use REST API calls for many of the GuardAPI functions. Providing a REST interface to the Guardium API simplifies integrating Guardium into your system.

For more information about GuardAPI functions with REST API capabilities, see [Guardium API A-Z Reference](#).

As shown in [Figure 1](#), take the following steps to set up your Guardium system for the REST API:

1. Use the command-line interface (CLI) to register the client ID from the collector side. Each client needs to be registered only once. The CLI returns a client secret for the client ID.
2. Use the curl command-line tool from the REST client to send a request for an access token along with the client secret to the Guardium appliance.
3. After the REST client is authorized, you can use the access token to call the supported GuardAPI functions.

Figure 1. Getting started with the REST API



Example use cases

A few examples of when you might use a REST API:

- I want the ability to dynamically get a small amount of audit data for a certain IP address without having to login to the Guardium GUI.
- I want to populate an existing group, so I can update my policy to prevent unauthorized access to sensitive information.
- I want to get a list of all users within a certain authorized access group.
- I want my application development team to help identify which sensitive tables to monitor.
- I want to script access to GuardAPIs without using "expect" scripting language, which requires me to code response text from the target system.

Calling REST APIs example

The following scenario describes how to use the `register_oauth_client` GuardAPI to register the client and then call a GuardAPI function from the REST client.

1. Register the application and get the client secret.

Access to the collector from the CLI, and run the following `grdapi` command to register the application, as shown:

```
example.yourdomain.com> grdapi register_oauth_client client_id=client1 grant_types="password"
ID=0
```

The application returns the client secret, as shown in the following example:

```
{"client_id": "client1", "client_secret": "b1f242a2-1e86-46d6-bf42-6298556c2eea", "grant_types": "password"}
ok
example.yourdomain.com>
```

Note: You need to register the application only once.

2. From the REST client, include the client secret in a curl request for the access token:

```
C:\tools\curl-7.57.0-win64-mingw\bin>curl -k -X POST -d "client_id=client1&client_secret=b1f242a2-1e86-46d6-bf42-6298556c2eea&grant_type=password&username=admin&password=*****" https://example.yourdomain.com:8443/oauth/token
```

Guardium returns the access token:

```
{"access_token": "29ff4bb4-e622-41cf-97d0-de695ebd756b", "token_type": "bearer", "expires_in": 10799, "scope": "read write"}
C:\tools\curl-7.57.0-win64-mingw\bin>
```

3. Use the access token to call a Guardium API function from the REST API. The following example calls the equivalent of the `list_datasource_by_id id=20000` function from the REST client.

```
C:\tools\curl-7.57.0-win64-mingw\bin>curl \
-k --header "Authorization: Bearer 29ff4bb4-e622-41cf-97d0-de695ebd756b" \
--include --header "Content-Type: application/json" \
-X GET https://example.yourdomain.com:8443/restAPI/datasource?id=20000
```

This REST API call returns the following information about the specified data source:

```
HTTP/1.1 200 OK
X-FRAME-OPTIONS: SAMEORIGIN
Set-Cookie: JSESSIONID=C7854CAF60CE7B3A6CD585A8173B3222; Path=/; Secure; HttpOnly
Cache-Control: max-age=86400
Expires: Tue, 16 Jan 2018 09:21:52 GMT
Access-Control-Allow-Methods: POST, GET, PUT, DELETE
Access-Control-Allow-Headers: authorization, origin, X-Requested-With, Content-Type, Accept
Access-Control-Max-Age: 18000
Content-Type: application/json; charset=UTF-8
Content-Length: 914
Date: Mon, 15 Jan 2018 09:21:52 GMT
Server: SQL Guard
[
  {
    "DatasourceId": "https://example.yourdomain.com:8443/restAPI/datasource?id=20000",
    "DatasourceTypeId": "13",
    "Name": "System (9.70.148.141)",
    "Description": "null",
    "Host": "9.70.148.141",
    "Port": "0",
```

```
"ServiceName": "",  
...  
"
```

Additional API examples

This example uses the POST verb to create a new data source:

```
curl -k --header "Authorization:Bearer 04ce5d90-8d89-4e9c-a060-ec94b4409a71" \  
--include --header "Content-Type: application/json" \  
-X POST --data '{"application":"Classifier","host":"192.168.1.54","name":"mydbserver","type":"TEXT:HTTPS"}' \  
https://192.168.1.10:8443/restAPI/datasource
```

This example uses GET to return the status of all installed applications:

```
curl -k --header "Authorization:Bearer da186a7e-488d-4cd2-a35b-094b3cc4af86" \  
--include --header "Content-Type: application/json" \  
-X GET https://192.168.1.10:8443/restAPI/applications
```

This example updates an existing data source by its ID (which is 20001):

```
curl -k --header "Authorization:Bearer 04ce5d90-8d89-4e9c-a060-ec94b4409a71" \  
--include --header "Content-Type: application/json" \  
-X PUT --data '{"id":20001,"description":"My database server."}' \  
https://192.168.1.10:8443/restAPI/update_datasource_by_id
```

This example deletes an application (1500):

```
curl -k --header "Authorization:Bearer 14da5202-f3c6-45d0-bc10-77604e6cede7" \  
--include --header "Content-Type: application/json" \  
-X DELETE --data '{"application_id": 1500}' https://192.168.1.10:8443/restAPI/applications
```

For information about which GuardAPI functions also have REST API calls, see [Guardium API A-Z Reference](#).

For more information about Guardium REST API error codes, see [Return Codes for Guardium REST APIs](#) in the IBM Support database.

Guardium API A- Z Reference

All of the Guardium GuardAPI commands, arranged alphabetically. Click the GuardAPI command for more information about that command. If the GuardAPI command has a REST API interface, the REST call is also provided.

List of GuardAPI and REST API Functions

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | G | H | I | J | K | L | M | |
| N | O | P | Q | R | S | I | U | V | W | X | Y | Z |

A

API commands beginning with A.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|---|---------------|--|-------------|
| add_action_to_fam_rule | Yes | addActionToFAMRule | POST |
| add_all_to_schedule | Yes | addAllToSchedule | POST |
| add_approved_stap_client | Yes | addApprovedClient | POST |
| add_assessment_datasource | Yes | addAssessmentDatasource | POST |
| add_assessment_datasource_group | Yes | addAssessmentDatasourceGroup | POST |
| add_assessment_test | Yes | addAssessmentTest | POST |
| add_assessment_test_by_dsid | Yes | addAssessmentTestByDsType | POST |
| add_autodetect_task | Yes | addAutoDetectTask | POST |
| add_available_test_notes | Yes | addAvailableTestNotes | POST |
| add_classifier_datasource | Yes | clsAddDatasource | POST |
| add_classifier_datasource_group | Yes | clsAddDataSourceGroup | POST |
| add_cluster | Yes | addCluster | POST |
| add_connection_properties | Yes | addConProperties | POST |
| add_custom_property_to_datasources_in_group | Yes | addCustomPropToDatasourcesInGroup | POST |
| add_custom_property_to_datasource_by_id | Yes | datasourceAddCustomProp | POST |
| add_custom_property_to_datasource_by_name | Yes | datasourceAddCustomProp | POST |
| add_datasource_to_entitlement_optimization | Yes | addDatasourceToEntitlementOptimization | PUT |
| add_datasource_to_group | Yes | addDatasource | POST |
| add_dm_to_profile | Yes | addDMToProfile | PUT |
| add_domain_to_universal_connector_allowed_domains | Yes | addDomainToUcAllowedDomains | POST |
| add_group_to_quick_search | No | | |
| add_ip_to_sg | Yes | addCollectorsIPtoGSecurityGroup | POST |
| add_mfa_exempt_users | Yes | addExemptUsers | PUT |
| add_objects_native_audit | Yes | enableNativeAuditOnObjects | POST |
| add_ranger_config | Yes | addConfig | POST |
| add_ranger_hdfs_config | Yes | addHDFSConfig | POST |

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|---|---------------|---------------------------|-------------|
| add_ranger_service | Yes | mapServiceToConfig | POST |
| add_receiver_to_rule_action | Yes | addReceiveToRuleAction | POST |
| add_stream | Yes | addStream | POST |
| add_threshold_to_rule | Yes | addRule | PUT |
| add_time_period | Yes | timePeriodAdd | POST |
| apply_rules_on_discoveredinstances | Yes | applyRulesToDIs | PUT |
| assign_analytic_case | Yes | assignAnalyticCase | PUT |
| assign_collectors | Yes | assignCollectors | PUT |
| assign_load_balancer_groups | No | | |
| assign_qr_condition_to_action | Yes | assignQrConditionToAction | POST |
| audit_process_run_status | Yes | AuditProcessRunStatus | GET |
| auto_execute_suggested_dependencies | No | | |

B

API commands beginning with B.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|---|---------------|--------------------|-------------|
| backup_cm_list_candidates | Yes | listCandidates | GET |
| backup_cm_set | Yes | setBackupCM | PUT |

C

API commands beginning with C.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|---|---------------|----------------------------------|-------------|
| cancel_distributed_report_target | No | | |
| change_cli_password | Yes | changeCliPassword | POST |
| change_monitor_value | Yes | changeMonitorValue | POST |
| change_rule_order | Yes | changeRuleOrder | PUT |
| change_to_microsoft | Yes | changeToMicrosoft | PUT |
| change_to_opensource | Yes | changeToOpensource | PUT |
| change_tracker_get_events | Yes | getHealthEvents | GET |
| change_tracker_get_params | Yes | getParam | GET |
| change_tracker_get_tasks | Yes | getTasks | GET |
| change_tracker_reset | Yes | reset | PUT |
| change_tracker_set_params | Yes | setParam | PUT |
| clear_cas_template_set | Yes | clearCasTemplateSet | PUT |
| clevix_bind | No | | |
| clone_assessment | Yes | cloneAssessment | POST |
| clone_cas_template_set | Yes | cloneCasTemplateSet | POST |
| clone_extraction_profile | Yes | cloneExtractionProfile | PUT |
| clone_policy | Yes | clonePolicy | POST |
| close_default_events | No | | PUT |
| configure_archive | Yes | configArchive | PUT |
| configure_data_streaming | Yes | dataStreaming | POST |
| configure_export | Yes | configExport | PUT |
| configure_mfa | Yes | configMfa | POST |
| configure_purge | Yes | configurePurge | PUT |
| configure_results_archive | Yes | configResultsArchive | PUT |
| configure_results_export | Yes | configResultsExport | POST |
| configure_system_backup | Yes | configBackup | POST |
| copy_key_file | Yes | copyKeyFile | PUT |
| copy_rule | Yes | copyRule | POST |
| copy_rules | Yes | copyRules | POST |
| create_adhoc_policy_analyzer | Yes | setSchedule | PUT |
| create ad hoc audit and run once | Yes | createAuditProcess | POST |
| create ad hoc audit and run with name | Yes | createAuditProcessWithReportName | POST |
| create_ad_hoc_audit_for_security_assessment | Yes | createAuditProcForSA | POST |
| create_alias | Yes | createAlias | POST |
| create_allowed_db | Yes | create | POST |
| create_api_parameter_mapping | Yes | addParamMappingForFunction | POST |
| create_assessment | Yes | addAssessment | POST |
| create_autodetect_process | Yes | createAutoDetectProcess | POST |
| create_aws_secrets_manager_config | Yes | createAwsSecretsManagerConfig | POST |
| create_cas_host_instance | Yes | createCasHostInstance | POST |
| create_cas_template | Yes | createCasTemplate | POST |
| create_cas_template_set | Yes | createCasTemplateSet | POST |
| create_classifier_action | Yes | actionAdd | POST |

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|--|---------------|----------------------------|-------------|
| create_classifier_document_rule | Yes | ruleDocumentAdd | POST |
| create_classifier_policy | Yes | policyAdd | POST |
| create_classifier_process | Yes | processAdd | POST |
| create_classifier_rule | Yes | ruleAdd | POST |
| create_cloudTitle | Yes | createCloudTitle | POST |
| create_cloud_datasource | Yes | createCloudDS | POST |
| create_computed_attribute | Yes | create | POST |
| create_constant_attribute | Yes | create | POST |
| create_custom_table_ldap_import | Yes | createLdapConfig | POST |
| create_cyberark_config | Yes | createCyberarkConfig | POST |
| create_datasource | Yes | create | POST |
| create_datasourceRef_by_id | Yes | createRef | POST |
| create_datasourceRef_by_name | Yes | createRef | POST |
| create_datasource_custom_property | Yes | createCustomProp | POST |
| create_datasource_group | Yes | createGroup | POST |
| create_datasource_groupRef_by_id | Yes | createRef | POST |
| create_datasource_groupRef_by_name | Yes | createRef | POST |
| create_db_user_mapping | Yes | create | POST |
| create_ef_mapping | Yes | createEfMapping | PUT |
| create_entry_location | Yes | addLocation | POST |
| create_fam_rule | Yes | createPolicyRule | POST |
| create_group | Yes | create | POST |
| create_hashicorp_config | Yes | createHashicorpConfig | POST |
| create_hierarchical_member_to_group_by_desc | Yes | addHMemberToGroup | POST |
| create_kafka_cluster | Yes | createCluster | POST |
| create_member_to_group_by_desc | Yes | addMemberToGroup | POST |
| create_member_to_group_by_id | Yes | addMemberToGroup | POST |
| create_member_to_group_DAMX_Standard_Activity | No | | |
| create_member_to_group_DAMX_Suspicious_Connections | No | | |
| create_online_report | Yes | createReportResult | POST |
| create_policy | Yes | createRuleSet | POST |
| create_qr_action | Yes | createQrAction | POST |
| create_qr_add_where | Yes | createQrAddWhere | POST |
| create_qr_add_where_by_id | Yes | createQrAddWhereById | POST |
| create_qr_condition | Yes | createQrCondition | POST |
| create_qr_definition | Yes | createQRdefinition | POST |
| create_qr_replace_element | Yes | createQrReplaceElement | POST |
| create_qr_replace_element_byId | Yes | createQrReplaceElementById | POST |
| create_quarantine_allowed_until | Yes | addQuarantineAllowedUntil | POST |
| create_quarantine_until | Yes | addQuarantineUntil | POST |
| create_role | Yes | createRole | POST |
| create_rule | Yes | createRule | POST |
| create_rule_action | Yes | actionAdd | POST |
| create_sql_configuration | Yes | createSqlConfiguration | POST |
| create_stap_inspection_engine | Yes | createStapInspectionEngin | POST |
| create_test_detail_exception | Yes | createNew | POST |
| create_test_exception | Yes | create | POST |
| create_user | Yes | createUser | POST |
| create_update_wkc_config | Yes | configureWkc | POST |
| create_user_hierarchy | Yes | create | POST |

D

API commands beginning with D.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|--|---------------|----------------------|-------------|
| datamart_copy_file_bundle | Yes | copyFileBundle | PUT |
| datamart_include_file_header | Yes | includeFileHeader | PUT |
| datamart_refresh_metadata | Yes | refreshMetadata | PUT |
| datamart_run_once_now | Yes | runOnceNow | PUT |
| datamart_set_active | Yes | setActive | PUT |
| datamart_set_date_format | Yes | setDateFormat | PUT |
| datamart_set_inactive | Yes | setInactive | PUT |
| datamart_update_copy_file_info | Yes | updateCopyFileInfo | PUT |
| datamart_validate_copy_file_info | Yes | validateCopyFileInfo | PUT |
| delete_adhoc_policy_analyzer | Yes | deleteSchedule | DELETE |
| delete_alerter_snmp_settings | Yes | deleteSnmpSettings | DELETE |
| delete_alias | Yes | deleteAlias | DELETE |

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|---|---------------|---------------------------------|-------------|
| delete_allowed_db_by_entry_id | Yes | delete_by_entry_id | DELETE |
| delete_allowed_db_by_user | Yes | delete_by_user | DELETE |
| delete_analytic_user_feedback | Yes | deleteUserFeedback | PUT |
| delete_api_parameter_mapping | Yes | removeParamMappingForFunction | DELETE |
| delete_approved_stap_client | Yes | removeApprovedClient | DELETE |
| delete_archive_configuration | Yes | deleteArchiveConfig | DELETE |
| delete_assessment | Yes | deleteAssessment | DELETE |
| delete_assessment_datasource | Yes | deleteAssessmentDatasource | DELETE |
| delete_assessment_datasource_group | Yes | deleteAssessmentDatasourceGroup | DELETE |
| delete_assessment_test | Yes | deleteAssessmentTest | DELETE |
| delete_audit_process | Yes | deleteAuditProcess | DELETE |
| delete_audit_process_result | Yes | deleteResults | DELETE |
| delete_autodetect_process | Yes | deleteAutodetectProcess | DELETE |
| delete_autodetect_scans_for_process | Yes | deleteAutoDetectScansForProcess | DELETE |
| delete_available_test_notes | Yes | deleteAvailableTestNotes | DELETE |
| delete_aws_secrets_manager_config | Yes | deleteAwsSecretsManagerConfig | DELETE |
| delete_cas_host | Yes | deleteCasHost | DELETE |
| delete_cas_host_instance | Yes | deleteCasHostInstance | DELETE |
| delete_cas_template | Yes | deleteCasTemplate | DELETE |
| delete_cas_template_set | Yes | deleteCasTemplateSet | DELETE |
| delete_classifier_action | Yes | actionDel | DELETE |
| delete_classifier_document_rule | Yes | ruleDocumentDel | DELETE |
| delete_classifier_policy | Yes | policyDel | DELETE |
| delete_classifier_process | Yes | processDel | DELETE |
| delete_classifier_rule | Yes | ruleDel | DELETE |
| delete_cluster | Yes | deleteCluster | DELETE |
| delete_computed_attribute | Yes | remove | DELETE |
| delete_constant_attribute | Yes | remove | DELETE |
| delete_custom_table_ldap_import | Yes | deleteLdapImport | DELETE |
| delete_cust_table_distribution_schedule | Yes | deleteSchedule | DELETE |
| delete_cyberark_config | Yes | deleteCyberarkConfig | DELETE |
| delete_datasourceRef_by_id | Yes | deleteRef | DELETE |
| delete_datasourceRef_by_name | Yes | deleteRef | DELETE |
| delete_datasource_by_id | Yes | delete | DELETE |
| delete_datasource_by_name | Yes | delete | DELETE |
| delete_datasource_configuration | No | | |
| delete_datasource_custom_property | Yes | deleteCustomProp | DELETE |
| delete_datasource_group | Yes | deleteGroup | DELETE |
| delete_datasource_groupRef_by_id | Yes | deleteRef | DELETE |
| delete_datasource_groupRef_by_name | Yes | deleteRef | DELETE |
| delete_db_user_mapping | Yes | delete | DELETE |
| delete_distributed_report_result_for_period | No | | |
| delete_ef_mapping | Yes | deleteEfMapping | DELETE |
| delete_entry_location | Yes | removeLocation | DELETE |
| delete_export_configuration | Yes | deleteExportConfig | DELETE |
| delete_group_by_desc | Yes | delete | DELETE |
| delete_group_by_id | Yes | delete | DELETE |
| delete_group_from_quick_search | No | | |
| delete_hashicorp_config | Yes | deleteHashicorpConfig | DELETE |
| delete_hierarchical_member_from_group_by_desc | Yes | removeHMemberFromGroup | DELETE |
| delete_imsccheckpoint_record | Yes | deleteIMSCheckpoint | DELETE |
| delete_inactive_stap | Yes | deleteInactiveStap | POST |
| delete_invalid_stap | No | | |
| delete_kafka_cluster | Yes | deleteCluster | DELETE |
| delete_member_from_group_by_desc | Yes | removeMemberFromGroup | DELETE |
| delete_member_from_group_by_id | Yes | removeMemberFromGroup | DELETE |
| delete_oauth_clients | No | | DELETE |
| delete_policy | Yes | deletePolicy | DELETE |
| delete_quarantine | Yes | deleteQuarantine | DELETE |
| delete_ranger_hdfs_config | Yes | deleteHDFSConfig | DELETE |
| delete_results_archive_configuration | Yes | deleteResultsArchiveConfig | DELETE |
| delete_results_export_configuration | Yes | deleteResultsExport | DELETE |
| delete_rule | Yes | removeRule | DELETE |
| delete_schedule | Yes | deleteSchedule | DELETE |
| delete_sql_configuration | Yes | removeSqlConfiguration | DELETE |
| delete_stap_inspection_engine | Yes | removeInspectionEngine | DELETE |
| delete_stream | Yes | deleteStream | DELETE |

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|---|---------------|---|-------------|
| delete_system_backup_configuration | Yes | deleteSystemBackup | DELETE |
| delete_test_detail_exception | Yes | deleteException | DELETE |
| delete_test_detail_exception_by_id | Yes | deleteExceptionById | DELETE |
| delete_test_exception | Yes | deleteException | DELETE |
| delete_test_exception_by_id | Yes | deleteException | DELETE |
| delete_user | Yes | deleteUser | DELETE |
| delete_user_hierarchy_by_entry_id | Yes | delete_by_entry_id | DELETE |
| delete_user_hierarchy_by_user | Yes | delete_by_user | DELETE |
| disable_advanced_threat_scanning | Yes | disableEagleEye | PUT |
| disable_auto_execute_suggested_dependencies | No | | |
| disable_big_data_interface | Yes | disable | DELETE |
| disable_datastream | Yes | disableStream | POST |
| disable_embed_eastern_font | No | | |
| disable_entitlement_optimization | Yes | disableEntitlementOptimization | PUT |
| disable_fam_crawler | Yes | disableFamCrawler | PUT |
| disable_health_analyzer | Yes | disableHealthAnalyzer | PUT |
| disable_ip_to_host_aliases | Yes | disableIpToHostAliases | PUT |
| disable_monitoring_ranger_service | Yes | disableService | PUT |
| disable_native_audit | Yes | disableNativeAudit | POST |
| disable_outliers_detection | Yes | disableOutliersDetection | PUT |
| disable_outliers_detection_agg | Yes | disableOutliersDetectionOnAgg | PUT |
| disable_outliers_detection_cross_cm_agg | Yes | disableOutliersDetectionOnAggCrossCm | PUT |
| disable_outliers_detection_cross_cm_collector | Yes | disableOutliersDetectionOnCollectorsCrossCM | PUT |
| disable_persistent_queue_universal_connector | Yes | disablePersistentQueue | GET |
| disable_policy_analyzer | Yes | stopAnalyzer | PUT |
| disable_purge | Yes | disablePurge | DELETE |
| disable_quick_search | Yes | disableQuickSearch | PUT |
| disable_riskspotter | Yes | disableRiskspotter | POST |
| disable_special_attributes | No | | PUT |
| disable_test_result_detail_string_setting | Yes | disableDetailStringSetting | POST |
| disable_threat_detection_use_case | Yes | disableUseCase | POST |
| disable_thread_finder | Yes | disableThreadFinder | PUT |
| discover_streams | Yes | discoverStreams | GET |
| display_external_stap_config | Yes | displayTapConfig | GET |
| display_stap_config | Yes | displayTapConfig | GET |

E

API commands beginning with E.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|--|---------------|---|-------------|
| edit_kafka_cluster | Yes | editKafka | PUT |
| enable_advanced_threat_scanning | Yes | enableEagleEye | PUT |
| enable_all_tls | No | | GET |
| enable_big_data_interface | Yes | enable | PUT |
| enable_datastream | Yes | enableStream | POST |
| enable_disable_ip_restriction | Yes | enableDisabledIPRestriction | POST |
| enable_disable_monitoring_streams | Yes | monitorStream | PUT |
| enable_embed_eastern_font | No | | |
| enable_entitlement_optimization | Yes | enableEntitlementOptimization | PUT |
| enable_fam_crawler | Yes | enableFamCrawler | PUT |
| enable_fips_tls | No | | GET |
| enable_health_analyzer | Yes | enableHealthAnalyzer | PUT |
| enable_health_traffic_job | Yes | enableTraffic | POST |
| enable_ip_to_host_aliases | Yes | enableIpToHostAliases | PUT |
| enable_latest_tls | No | | GET |
| enable_monitoring_ranger_service | Yes | enableService | PUT |
| enable_native_audit | Yes | enableNativeAudit | POST |
| enable_outliers_detection | Yes | enableOutliersDetection | PUT |
| enable_outliers_detection_agg | Yes | enableOutliersDetectionOnAgg | PUT |
| enable_outliers_detection_cross_cm_agg | Yes | enableOutliersDetectionCrossCMOnAgg | PUT |
| enable_outliers_detection_cross_cm_collector | Yes | enableOutliersDetectionCrossCMOnCollector | PUT |
| enable_persistent_queue_universal_connector | Yes | enablePersistentQueue | GET |
| enable_policy_analyzer | Yes | startAnalyzer | PUT |
| enable_quick_search | Yes | enableQuickSearch | PUT |
| enable_riskspotter | Yes | enableRiskspotter | POST |
| enable_special_attributes | No | | PUT |
| enable_strong_cli_password | Yes | enableStrongPassword | POST |

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|--|---------------|----------------------|-------------|
| enable_threat_detection_use_case | Yes | enableUseCase | POST |
| enable_threat_finder | Yes | enableThreadFinder | PUT |
| encrypt_value | Yes | encryptValue | POST |
| execute_appUserTranslation | Yes | execute | PUT |
| execute_assessment | Yes | execute | PUT |
| execute_auditProcess | Yes | execute | PUT |
| execute_autodetect_process | Yes | runAutoDetectProcess | PUT |
| execute_cls_process | Yes | execute | PUT |
| execute_flatLogProcess | Yes | execute | PUT |
| execute_incidentGenProcess | Yes | execute | PUT |
| execute_incidentGenProcess_byDetails | Yes | execute | PUT |
| execute_ldap_user_import | Yes | importLdapUsers | POST |
| execute_populateGroupFromQuery | Yes | execute | PUT |
| export_certificate | Yes | exportCertificate | PUT |
| export_config | Yes | exportConfig | PUT |
| export_definition | No | | PUT |
| export_log_files | Yes | exportlogfiles | POST |
| export_transfer_key | Yes | cp_key | POST |

F

API commands beginning with F.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|---|---------------|--------------------|-------------|
| f5_add_apps_config | No | | POST |
| f5_add_data_params | No | | POST |
| f5_delete_apps_config | No | | DELETE |
| f5_delete_data_params | No | | DELETE |
| f5_list_apps_config | No | | GET |
| f5_list_data_params | No | | GET |
| f5_update_data_params | No | | PUT |
| fipsmode | Yes | ModifyFipsmode | POST |
| flatten_hierarchical_groups | Yes | execute | PUT |

G

API commands beginning with G.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|--|---------------|----------------------------------|-------------|
| generate_ssl_key_universal_connector | Yes | generateSSLKeyUniversalConnector | POST |
| generate_transfer_key | Yes | regenkeys | POST |
| getFieldsTitles | Yes | getFieldsTitles | GET |
| getOAuthTokenExpirationTime | No | | GET |
| get_all_modifiable_guard_params | Yes | getAllModifiableGuardParams | GET |
| get_assessment_result | Yes | getAssessmentResult | GET |
| get_clusters | Yes | getAllClusters | GET |
| get_cluster_members | Yes | getClusterMembers | GET |
| get_datamart_info | No | | PUT |
| get_datasource_custom_properties | Yes | listCustomProps | GET |
| get_debug_level | No | | |
| get_definitions_data_sets | Yes | getDefinitionTypes | GET |
| get_definitions_items | Yes | getDefinitionsItems | GET |
| get_distributed_report_target_info | No | | |
| get_entitlement_optimization_info | Yes | getEntitlementOptimizationInfo | PUT |
| get_expiration_date_for_restored_day | Yes | getExpirationForRestoredDate | GET |
| get_extraction_profile_info | Yes | listExtractionProfiles | GET |
| get_fam_crawler_info | Yes | getFamCrawlerInfo | GET |
| get_flatLogProcessType | Yes | getFlatLogProcessType | GET |
| get_guard_param | Yes | getGuardParam | GET |
| get_hadoop_cluster_status | Yes | getHadoopClusterStatus | GET |
| get_health_traffic_status | Yes | getTrafficFrequency | GET |
| get_inapplicable_test_result_status | Yes | getInapplicableTestResult | GET |
| get_insights_agent_config | Yes | getInsightsAgentParams | GET |
| get_ip_restriction_config | Yes | getConfiguration | GET |
| get_ip_to_alias_overwrites | Yes | getIpToAliasOverwrites | GET |
| get_ip_to_alias_selected | Yes | getIpToAliasSelected | GET |
| get_istap_config | Yes | get_istap_config | GET |
| get_istap_status | Yes | get_istap_status | GET |
| get_job_process_concurrency_limit | No | | |

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|--|---------------|---------------------------------------|-------------|
| get_kafka_clusters | Yes | getClusters | GET |
| get_load_balancer_load_map | No | | |
| get_load_balancer_params | No | | |
| get_mfa_configuration | Yes | getActiveConfig | GET |
| get_native_audit_collectors | Yes | getCollectorsList | GET |
| get_native_audit_configurations | Yes | getNativeAuditConfiguration | GET |
| get_native_audit_objects | Yes | getNativeObjectList | GET |
| get_outliers_detection_info | No | | |
| get_policy_analyzer_status | Yes | getStatus | GET |
| get_purge_batch_size | No | | GET |
| get_quick_search_info | Yes | getQuickSearchInfo | GET |
| get_ranger_config | Yes | getAmbariConfigByClusterName | GET |
| get_ranger_hdfs_config | Yes | getHDFSConfig | GET |
| get_ranger_services_status | Yes | monitorServices | GET |
| get_registered_units | Yes | getRegisteredUnits | GET |
| get_secured_protocols_info | No | | GET |
| get_solr_cluster_info | No | | |
| get_solr_errors | No | | |
| get_solr_status | No | | |
| get_solr_status_extended | No | | |
| get_streams | Yes | getStreams | GET |
| get_test_result_detail_string_setting | Yes | getDetailStringSetting | GET |
| get_threat_detection_use_case_info | Yes | getCaseTypesInfo | GET |
| get_unit_data | Yes | getUnitData | GET |
| get_unit_pinger | No | | GET |
| get_universal_connector_allowed_domains | Yes | getUcDomainsAllowedDomains | GET |
| get_universal_connector_status | Yes | getUniversalConnectorStatus | GET |
| get_va_summary_key | Yes | getVASummaryKey | GET |
| get_wkc_config | Yes | getWkcConfig | GET |
| get_ztap_logging_config | Yes | getZtapLoggingConfig | GET |
| gim_assign_bundle_or_module_to_client_by_version | Yes | assignBundleOrModuleToClientByVersion | PUT |
| gim_assign_latest_bundle_or_module_to_client | Yes | assignLatestBundleOrModuleToClient | PUT |
| gim_cancel_install | Yes | cancelInstall | PUT |
| gim_cancel_uninstall | Yes | cancelUninstall | PUT |
| gim_get_available_modules | Yes | getAvailableModules | GET |
| gim_get_client_last_event | Yes | listClientStatus | GET |
| gim_get_global_param | No | | |
| gim_get_modules_running_status | No | | |
| gim_list_bundles | Yes | listBundles | GET |
| gim_list_client_modules | Yes | listClientModules | GET |
| gim_list_client_params | Yes | listClientParams | GET |
| gim_list_mandatory_params | No | | GET |
| gim_list_registered_clients | Yes | listRegisteredClients | GET |
| gim_list_unused_bundles | Yes | listUnusedBundles | GET |
| gim_load_package | Yes | loadPackage | GET |
| gim_remote_activation | No | | |
| gim_remove_bundle | Yes | removeBundleByPackageName | DELETE |
| gim_reset_client | No | | |
| gim_schedule_install | Yes | scheduleInstall | PUT |
| gim_schedule_uninstall | Yes | scheduleUninstall | PUT |
| gim_set_diagnostics | No | | |
| gim_set_global_param | No | | |
| gim_unassign_client_module | Yes | unassignClientModule | PUT |
| gim_uninstall_module | Yes | uninstallModule | DELETE |
| gim_update_client_params | Yes | updateClientParams | PUT |
| grant_role_to_object_by_id | Yes | addRole | PUT |
| grant_role_to_object_by_Name | Yes | addRole | PUT |

H

API commands beginning with H.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|-----------------------------|---------------|--------------------|-------------|
| health_info | Yes | getHealthInfo | GET |

I

API commands beginning with I.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|---|---------------|--------------------------|-------------|
| import_definitions | Yes | definitionsImport | POST |
| insights_registration | Yes | registerCmToInsights | POST |
| insights_unregistration | Yes | unregisterCmFromInsights | DELETE |

K

API commands beginning with K.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|--------------------------------------|---------------|--------------------|-------------|
| kill_running_process | Yes | KillRunningProcess | POST |

L

API commands beginning with L.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|---|---------------|--------------------------------|-------------|
| list_adhoc_policy_analyzer | Yes | getSchedule | GET |
| list_aliases | Yes | listAliases | GET |
| list_allowed_db_by_user | Yes | list_by_user | GET |
| list_all_reports | Yes | listAllReports | GET |
| list_approved_stap_client | Yes | listApprovedClients | GET |
| list_assessments | Yes | listAssessments | GET |
| list_assessment_tests | Yes | listAssessmentTests | GET |
| list_associated_stap_mu_groups | Yes | listAssociatedStapMUGroups | GET |
| list_audit_processes | Yes | listAuditProcesses | GET |
| list_autodetect_processes | Yes | listAutoDetectProcesses | GET |
| list_autodetect_tasks_for_process | Yes | listAutoDetectTasksForProcess | GET |
| list_available_tests | Yes | listAvailableTests | GET |
| list_available_test_notes | Yes | listAvailableTestNotes | GET |
| list_aws_secrets_manager_config | Yes | listAwsSecretsManagerConfigs | GET |
| list_cas_hosts | Yes | listCasHosts | GET |
| list_cas_host_instances | Yes | listCasHostInstances | GET |
| list_cas_templates | Yes | listCasTemplates | GET |
| list_cas_template_sets | Yes | listCasTemplateSets | GET |
| list_classifier_policy | Yes | policyList | GET |
| list_classifier_process | Yes | processList | GET |
| list_cloud_datasource_by_name | Yes | readCloudDS | GET |
| list_compatibility_modes | Yes | listCompatibilityModes | GET |
| list_computed_attribute | Yes | list_computed_attribute | GET |
| list_custom_table_ldap_imports | Yes | listLdapImports | GET |
| list_cyberark_config | Yes | listCyberarks | GET |
| list_datasourceRef_by_id | Yes | readRef | GET |
| list_datasourceRef_by_name | Yes | readRef | GET |
| list_datasource_by_id | Yes | read | GET |
| list_datasource_by_name | Yes | read | GET |
| list_datasource_groupRef_by_id | Yes | readRef | GET |
| list_datasource_groupRef_by_name | Yes | readRef | GET |
| list_datasource_groups | Yes | listDatasourceGroups | GET |
| list_datasource_group_hierarchy | Yes | listDataSourceToGroupHierarchy | GET |
| list_datasource_group_members | Yes | listDataSources | GET |
| list_db_drivers | Yes | listDbDrivers | GET |
| list_db_drivers_by_details | Yes | listDbDriversByDetails | GET |
| list_db_user_mapping | Yes | list | GET |
| list_ef_mapping | Yes | listEfMapping | GET |
| list_ef_report | Yes | listAllReports | GET |
| list_engine_config | Yes | listEngineConfig | GET |
| list_entry_location | Yes | readLocation | GET |
| list_existing_job_dependencies | No | | |
| list_expiration_dates_for_restored_days | Yes | getExpirationForRestoredDate | GET |
| list_groups | Yes | listGroups | GET |
| list_group_by_desc | Yes | read | GET |
| list_group_by_id | Yes | read | GET |
| list_group_members_by_desc | Yes | listMembers | GET |
| list_group_members_by_id | Yes | listMembers | GET |
| list_hashicorp_config | Yes | listHashicorpConfigs | GET |
| list_health_node | Yes | getHealthNodes | GET |
| list_imscheckpoint_records | Yes | listIMSCheckpoints | GET |
| list_inspection_engines | Yes | listInspectionEngines | GET |
| list_installed_policies | Yes | listInstalledPolicies | GET |

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|--|---------------|--------------------------------|-------------|
| list_managed_units | Yes | listManagedUnits | GET |
| list_members_of_groups_by_desc | Yes | listGroupMembersByDesc | GET |
| list_members_of_groups_by_id | Yes | listGroupMembersById | GET |
| list_oauth_clients | No | | GET |
| list_parameter_names_by_report_name | Yes | listParameterNamesByReportName | GET |
| list_param_mapping_for_function | No | | GET |
| list_policy | Yes | listPolicy | GET |
| list_policy_fam_rule | Yes | policyRulesList | GET |
| list_policy_rules | Yes | listPolicyRules | GET |
| list_qr_action | Yes | listQrAction | GET |
| list_qr_add_where | Yes | listQrAddWhere | GET |
| list_qr_add_where_by_id | Yes | listQrAddWhereById | GET |
| list_qr_condition | Yes | listQrCondition | GET |
| list_qr_condition_to_action | Yes | listQrConditionToAction | GET |
| list_qr_definitions | Yes | listQRdefinition | GET |
| list_qr_replace_element | Yes | listQrReplaceElement | GET |
| list_qr_replace_element_byId | Yes | listQrReplaceElementById | GET |
| list_quick_search_groups | No | | |
| list_ranger_configs | Yes | listAmbariConfigs | GET |
| list_ranger_hdfs_config | Yes | listHDFSConfig | GET |
| list_ranger_staps | Yes | listOfSTAPs | GET |
| list_ready_files | No | | |
| list_roles | Yes | listRoles | GET |
| list_roles_granted_to_object_by_id | Yes | read | GET |
| list_roles_granted_to_object_by_Name | Yes | read | GET |
| list_rules_with_threshold | Yes | getListRulesWithThresholds | GET |
| list_running_processes | Yes | ListRunningProcesses | GET |
| list_scheduler_jobs | No | | |
| list_schedules | Yes | listTriggers | GET |
| list_staps | Yes | listActiveStaps | GET |
| list_stap_verification_results | Yes | listStapVerificationAllResults | GET |
| list_test_detail_exception | Yes | listExceptions | GET |
| list_test_exception | Yes | listExceptions | GET |
| list_test_exception_by_id | Yes | listExceptions | GET |
| list_users | Yes | listUsers | GET |
| list_user_hierarchy_by_parent_user | Yes | list_by_parent_user | GET |
| list_user_roles | Yes | listUserRoles | GET |
| list_utilization_thresholds | No | | GET |
| load_all_packages | No | | |
| load_mongodb | No | | |
| load_mongodb_by_datasource | No | | |
| local_disable_big_data_intelligence | Yes | localDisableSonar | PUT |
| local_enable_big_data_interface | Yes | localEnable | PUT |

M

API commands beginning with M.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|---|---------------|-------------------------|-------------|
| make_bundle_with_uploaded_kernel_module | No | | |
| make_primary_cm | Yes | switchCMAPIServer | POST |
| migrate_stap_config | Yes | migrateTapConfig | PUT |
| modify_autodetect_process | Yes | modifyAutodetectProcess | PUT |
| modify_ef_mapping | Yes | modifyEfMapping | PUT |
| modify_ef_sql_mode | Yes | modifyEfSQLMode | PUT |
| modify_guard_param | Yes | updateGuardParam | POST |
| modify_oauth_validity | No | | PUT |
| modify_schedule | Yes | modifyTrigger | PUT |
| modify_va_summary_key | Yes | modifyKey | PUT |
| must_gather | Yes | startGatherApi | PUT |

N

API commands beginning with N.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|-------------------------------------|---------------|--------------------|-------------|
| non_credential_scan | No | | PUT |
| nscd | No | | |

P

API commands beginning with P.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|---|---------------|-------------------------|-------------|
| patch_cleanup | Yes | cleanup | PUT |
| patch_install | Yes | install | PUT |
| pause_or_resume_job | Yes | pauseOrResumeJob | PUT |
| pause_or_resume_scenarios | Yes | pauseOrResumeScenarios | PUT |
| policy_fam_rule_delete | Yes | deletePolicyRule | DELETE |
| policy_install | Yes | install | POST |
| policy_uninstall | Yes | uninstallPolicy | POST |
| populateMembersForGroup | Yes | populateMembersForGroup | GET |
| populate_from_dependencies | No | | POST |
| populate_group_from_query | Yes | addPopulateFromQuery | POST |
| proxy | Yes | proxyConfig | |
| pull_external_stap_keystore | No | | PUT |
| push_insights_trust | Yes | pushInsightsTrust | PUT |
| push_parameter_to_mu | Yes | pushGuardParamToMU | POST |

Q

API commands beginning with Q.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|------------------------------|---------------|--------------------|-------------|
| quick_search | Yes | quickSearch | POST |

R

API commands beginning with R.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|--|---------------|---|-------------|
| reboot_image_universal_connector | Yes | rebootUniversalConnectorImage | GET |
| refresh_quick_search_groups | No | | |
| refresh_stap_info | Yes | refreshStap | GET |
| register_oauth_client | No | | POST |
| register_oauth_internal_client | No | | |
| register_unit | Yes | registerUnit | POST |
| reinstall_policy | Yes | reinstallPolicy | POST |
| reinstall_policy_rule | Yes | reinstallPolicyRule | PUT |
| remove_all_from_schedule | Yes | removeAllFromSchedule | POST |
| remove_all_qr_replace_elements | Yes | removeAllQrReplaceElements | DELETE |
| remove_all_qr_replace_elements_by_id | Yes | removeAllQrReplaceElementsById | DELETE |
| remove_classifier_datasource | Yes | clsRemoveDatasource | DELETE |
| remove_classifier_datasource_group | Yes | clsRemoveDatasourceGroup | DELETE |
| remove_connection_properties | Yes | removeConProperties | DELETE |
| remove_custom_property_from_datasources_in_group | Yes | removeCustomPropFromDatasourcesInGroup | POST |
| remove_custom_property_from_datasource_by_id | Yes | datasourceRemoveCustomProp | POST |
| remove_custom_property_from_datasource_by_name | Yes | datasourceRemoveCustomProp | POST |
| remove_datasource_configuration_from_collector | No | | |
| remove_datasource_from_entitlement_optimization | Yes | removeDatasourceFromEntitlementOptimization | PUT |
| remove_datasource_from_group | Yes | removeDatasource | POST |
| remove_dm_from_profile | Yes | removeDMFromProfile | DELETE |
| remove_domain_from_universal_connector_allowed_domains | Yes | removeDomainFromUcAllowedDomains | DELETE |
| remove_extraction_profile | Yes | removeExtractionProfile | DELETE |
| remove_members_of_groups_by_desc | Yes | deleteMembers | DELETE |
| remove_members_of_groups_by_id | Yes | deleteMembers | DELETE |
| remove_mfa_exempt_users | Yes | removeExemptUsers | DELETE |
| remove_objects_native_audit | Yes | disableNativeAuditOnObjects | POST |
| remove_populate_group_from_query | Yes | removePopulateByQuery | DELETE |
| remove_qr_action | Yes | removeQrAction | DELETE |
| remove_qr_add_where_by_id | Yes | removeQrAddWhereById | DELETE |
| remove_qr_condition | Yes | removeQrCondition | DELETE |
| remove_qr_definition | Yes | removeQRdefinition | DELETE |
| remove_qr_replace_element_by_id | Yes | removeQrReplaceElementById | DELETE |
| remove_ranger_config | Yes | deleteConfig | DELETE |
| remove_ranger_service | Yes | deleteService | DELETE |
| remove_threshold_from_rule | Yes | deleteRule | PUT |
| replace_active_profile | Yes | replaceProfile | POST |
| reregister_agg_collector | No | | |
| rerun_datamart | No | | |

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|---|---------------|-----------------------------|-------------|
| rerun_distributed_report | No | | |
| reset_unit_utilization_data | Yes | resetUnit | PUT |
| reset_va_summary_by_id | Yes | resetById | PUT |
| reset_va_summary_by_key | Yes | resetByKey | PUT |
| restart_all_managed_units | No | | |
| restart_cloud_instance | Yes | restartInstance | POST |
| restart_job_queue_listener | Yes | execute | PUT |
| restart_solr | No | | |
| restart_stap | Yes | reinitializeBuffer | PUT |
| restart_unit_pinger | No | | PUT |
| restore_units_after_bad_shift | No | | |
| rest_export_definition | Yes | definitionsExport | POST |
| retreiveUpdatedUsers | Yes | retreiveUpdatedUsers | GET |
| retrieveApiParameters | Yes | retrieveApiParameters | GET |
| retrieveAPIs | Yes | retrieveAPI | GET |
| revokeOAuthClient | Yes | revokeOAuthClient | DELETE |
| revokeOAuthToken | No | | DELETE |
| revoke_ignore_stap | Yes | unIgnoreStap | POST |
| revoke_role_from_object_by_id | Yes | removeRole | DELETE |
| revoke_role_from_object_by_Name | Yes | removeRole | DELETE |
| riskspotter_set_config | Yes | setRiskspotterConfiguration | POST |
| rule_info_from_policy | Yes | ruleInfoFromPolicy | GET |
| run_custom_table_ldap_import | Yes | runLdapImport | POST |
| run_database_instance_discovery | Yes | runDBInstanceDiscovery | POST |
| run_diagnostics | Yes | runDiagnostics | PUT |
| run_populate_group_from_query | Yes | runPopulateByQuery | POST |
| run_universal_connector | Yes | runLocalUniversalConnector | GET |

S

API commands beginning with S.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|--|---------------|------------------------------------|-------------|
| save_datasource_configuration_on_collector | No | | |
| schedule_generate_mongo_filter_job | Yes | scheduleGenerateMongoFilterJob | POST |
| schedule_job | Yes | scheduleJob | PUT |
| sched_cust_table_distribution | Yes | scheduleDistribution | PUT |
| search | Yes | search | GET |
| secure_settings | Yes | secureSettings | |
| session_inference_control | Yes | controlSessionInference | POST |
| session_inference_setup | Yes | setupSessionInference | PUT |
| setOAuthTokenExpirationTime | No | | PUT |
| set_alerter_settings | Yes | updateAlerterSettings | POST |
| set_alerter_smtp_settings | Yes | updateSmtpSettings | POST |
| set_alerter_snmp_settings | Yes | updateSnmpSettings | POST |
| set_certificate_host_validation | Yes | setHostValidation | PUT |
| set_debug_level | No | | |
| set_distributed_report_target | No | | |
| set_enterprise_search_options | No | | |
| set_entitlement_datasource_parameter | Yes | setEntitlementDatasourceParameter | PUT |
| set_expiration_date_for_restored_day | Yes | setExpirationForRestoredDate | PUT |
| set_flatLogProcessType | Yes | setFlatLogProcessType | PUT |
| set_health_traffic_job_interval | Yes | setFrequency | POST |
| set_import | Yes | setImport | PUT |
| set_inapplicable_test_result_status | Yes | setInapplicableTestResult | POST |
| set_ip_to_alias_overwrites | Yes | setIpToAliasOverwrites | PUT |
| set_ip_to_alias_selected | Yes | setIpToAliasSelected | PUT |
| set_job_process_concurrency_limit | No | | |
| set_ktap_debug | Yes | setKtapDebug | PUT |
| set_load_balancer_param | No | | |
| set_outliers_detection_demo_mode | Yes | setOutlierDetectionPocMode | PUT |
| set_outliers_detection_parameter | No | | |
| set_outliers_detection_to_factory_settings | Yes | setOutlierDetectionFactorySettings | PUT |
| set_outliers_user_detection_mode | Yes | setOutliersDetectionUserMode | PUT |
| set_populate_group_from_query_schedule | Yes | updateImportFromQuerySchedule | PUT |
| set_purge_batch_size | No | | PUT |
| set_stap_debug | Yes | setStapDebug | PUT |
| set_universal_connector_log_level | Yes | setUniversalConnectorLogLevel | POST |

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|--|---------------|-----------------------------|-------------|
| set_user_roles | Yes | setUserRoles | PUT |
| set_ztap_logging_config | Yes | setZtapLoggingConfig | PUT |
| show_alerter_settings | Yes | showAlerterSettings | GET |
| show_alerter_smtp_settings | Yes | showSmtpSettings | GET |
| show_alerter_snmp_settings | Yes | showSnmpSettings | GET |
| show_alerter_status | Yes | showAlterStatus | GET |
| show_autodetect_process_status | Yes | showAutoDetectProcessStatus | GET |
| show_backup_cm_ip | Yes | shoMUSecondaryCMIP | GET |
| show_maximum_query_duration | Yes | ShowMaxQueryDuration | GET |
| show_universal_connector_plugins | Yes | showLogstashPlugins | GET |
| solr_repair_analysis | No | | |
| start_istap_monitor | Yes | start_istap_monitor | PUT |
| stop_audit_process | Yes | stopAuditProcess | PUT |
| stop_autodetect_process | Yes | stopAutoDetectProcess | PUT |
| stop_istap_monitor | Yes | end_istap_monitor | PUT |
| stop_restart_alerter | Yes | stopRestartAlerter | POST |
| stop_solr | No | | |
| stop_universal_connector | Yes | stopLocalUniversalConnector | POST |
| store_maximum_query_duration | Yes | StoreMaxQueryDuration | PUT |
| store_sql_credentials | Yes | sendSqlConfiguration | POST |
| store_stap_approval | Yes | storeStapApproval | POST |
| switch_outliers_user_mode | No | | PUT |

T

API commands beginning with T.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|---|---------------|-------------------------|-------------|
| test_datasource_connection | Yes | testConnection | POST |
| test_hashicorp_connection | Yes | testHashicorpConnection | POST |
| test_solr | No | | |
| test_solr_cluster_status | No | | |
| test_solr_connectivity | No | | |
| test_solr_hardware_requirements | No | | |

U

API commands beginning with U.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|---|---------------|-------------------------------|-------------|
| unassign_load_balancer_groups | No | | |
| unassign_qr_condition_from_action | Yes | unassignQrConditionFromAction | DELETE |
| uninstall_policy_rule | Yes | uninstallPolicyRule | DELETE |
| universal_connector_disable_metrics | Yes | updateMetricsSetting | POST |
| universal_connector_enable_metrics | Yes | updateMetricsSetting | POST |
| universal_connector_keystore_add | Yes | addWithOverrideKeystoreKey | POST |
| universal_connector_keystore_list | Yes | listKeystoreKeys | GET |
| universal_connector_keystore_remove | Yes | removeKeystoreKey | DELETE |
| universal_connector_troubleshooting | Yes | troubleshooting | GET |
| universal_connector_update_proxy | Yes | ucUpdateProxy | POST |
| unregister_unit | Yes | unRegisterUnit | POST |
| unschedule_datamart | Yes | unScheduleDatamart | DELETE |
| update_alias | Yes | updateAlias | PUT |
| update_assessment | Yes | updateAssessment | PUT |
| update_assessment_test | Yes | updateAssessmentTest | PUT |
| update_aws_secrets_manager_config | Yes | updateAwsSecretsManagerConfig | PUT |
| update_cas_host_instance | Yes | updateCasHostInstance | PUT |
| update_cas_template | Yes | updateCasTemplate | PUT |
| update_classifier_action | Yes | actionUpd | PUT |
| update_classifier_document_rule | Yes | ruleDocumentUpd | PUT |
| update_classifier_log_level | Yes | updateLogLevel | PUT |
| update_classifier_policy | Yes | policyUpd | PUT |
| update_classifier_process | Yes | processUpd | PUT |
| update_classifier_rule | Yes | ruleUpd | PUT |
| update_cloud_datasource | Yes | updateCloudDS | PUT |
| update_computed_attribute | Yes | update | PUT |
| update_constant_attribute | Yes | update | PUT |
| update_custom_table_ldap_import | Yes | updateLdapConfig | PUT |
| update_cyberark_config | Yes | updateCyberarkConfig | PUT |

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|---|---------------|--|-------------|
| update_datamart | Yes | updateDatamart | PUT |
| update_datamart_copy_file_threadpool_params | Yes | updateDatamartCopyFileThreadpoolParameters | PUT |
| update_datasource_by_id | Yes | update | PUT |
| update_datasource_by_name | Yes | update | PUT |
| update_datasource_credentials_in_group | Yes | changeCredentials | PUT |
| update_datasource_custom_property | Yes | updateCustomProp | PUT |
| update_datasource_group | Yes | updateGroup | PUT |
| update_engine_config | Yes | updateEngineConfig | PUT |
| update_entry_location | Yes | updateLocation | PUT |
| update_external_stap_config | Yes | updateTapConfig | PUT |
| update_group_by_desc | Yes | updateGroup | PUT |
| update_group_by_id | Yes | update | PUT |
| update_hashicorp_config | Yes | updateHashicorpConfig | PUT |
| update_insights_agent_config | Yes | updateInsightsAgentParams | PUT |
| update_insights_registration_config | Yes | updateInsightsRegistrationConfig | PUT |
| update_ip_restriction_allowlist | Yes | updateIpList | PUT |
| update_istap_config | Yes | update_istap_config | PUT |
| update_managed_units_ping_time | Yes | updateUnitPingTimestamp | PUT |
| update_policy | Yes | updatePolicy | PUT |
| update_policy_analyzer_interval | Yes | updateInterval | PUT |
| update_qr_action | Yes | updateQrAction | PUT |
| update_qr_add_where_by_id | Yes | updateQrAddWhereById | PUT |
| update_qr_condition | Yes | updateQrCondition | PUT |
| update_qr_definition | Yes | updateQRdefinition | PUT |
| update_qr_replace_element_byId | Yes | updateQrReplaceElementById | PUT |
| update_quarantine_allowed_until | Yes | updateQuarantineAllowedUntil | PUT |
| update_quarantine_until | Yes | updateQuarantineUntil | PUT |
| update_ranger_config | Yes | updateConfig | PUT |
| update_ranger_hdfs_config | Yes | updateHDFSConfig | POST |
| update_ranger_service | Yes | updateService | PUT |
| update_rule | Yes | updateRule | PUT |
| update_shared_secret | No | | |
| update_stap_config | Yes | updateTapConfig | PUT |
| update_test_detail_exception | Yes | update | PUT |
| update_test_exception | Yes | update | PUT |
| update_threshold_in_rule | Yes | updateRuleThreshold | PUT |
| update_user | Yes | updateUser | PUT |
| update_user_db | Yes | update | PUT |
| update_utilization_thresholds | No | | PUT |
| upload_custom_data | Yes | uploadDate | POST |

V

API commands beginning with V.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|---|---------------|----------------------------|-------------|
| venafi_import | Yes | importVenafi | PUT |
| verify_cyberark_access | Yes | verifyCyberarkAccess | GET |
| verify_stap_inspection_engine_with_sequence | Yes | verifyInspectionEngineHost | POST |

W

API commands beginning with W.

| GuardAPI function name | REST enabled? | REST resource name | REST method |
|--|---------------|-----------------------|-------------|
| wkc_refresh_external_pwd | Yes | refreshWkcExternalPwd | POST |

add_action_to_fam_rule

This command adds an action to an existing FAM rule.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/addActionToFAMRule
```

GuardAPI syntax

```
add_action_to_fam_rule parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|---|
| actionName | String | Required. The action taken when the rule criteria are met. Valid values: <ul style="list-style-type: none">• <i>Alert and audit</i>: Send an alert directly generated from the sniffer with specific behavior, and log the event.• <i>Audit only</i>: Log the event in GDM tables• <i>Block, log violation, and audit</i>: Block access to the object, log a policy violation, and log the event. A blocking action requires an alert configuration as well.• <i>Ignore</i>: No action taken.• <i>Log as violation and audit</i>: Log this as a policy violation and log the event. |
| alertReceiver | String | AlertReceiver is any user of the appliance like admin, etc. |
| classDestination | String | For valid values, call add_action_to_fam_rule from the command line with --help=true . |
| command | String | The command name to be included in the rule. For valid values, call add_action_to_fam_rule from the command line with --help=true . |
| commandGroup | String | Name of command group to be included in the rule. |
| commandGroupId | Integer | ID of command group to be included in the rule. |
| messageTemplate | String | Name of message template. For valid values, call add_action_to_fam_rule from the command line with --help=true . |
| notificationType | String | For valid values, call add_action_to_fam_rule from the command line with --help=true . |
| policyName | String | Required. Valid values: For valid values, call add_action_to_fam_rule from the command line with --help=true . |
| ruleName | String | Required. Rule that is getting modified with this command. |

Related concepts

- [FAM discovery and classification in Windows and UNIX-Linux file servers](#)
- [Using rules for file activity policies](#)

Related reference

- [create_policy](#)
- [delete_policy](#)
- [enable_fam_crawler](#)
- [create_fam_rule](#)
- [disable_fam_crawler](#)
- [get_fam_crawler_info](#)
- [list_policy_fam_rule](#)
- [policy_fam_rule_delete](#)

add_all_to_schedule

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/add_all_to_schedule
```

GuardAPI syntax

```
add_all_to_schedule parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

add_approved_stap_client

This command adds an approved database whose S-TAP® is allowed to access and communicate with the Guardium® system.

Prerequisite: `grdapib store_stap_approval=1`.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/approved_stap_client
```

GuardAPI syntax

```
add_approved_stap_client parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| stapHost | String | Required. The host name or IP address of the database server on which the S-TAP is installed. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To enable communication between the Guardium system and S-TAPs on the database with the IP address 9.148.116.204:

```
grdapib add_approved_stap_client stapHost=9.148.116.204
```

Related tasks

- [Allow \(approve\) S-TAP connection to Guardium \(S-TAP Certification\)](#)

Related reference

- [S-TAP and inspection engine APIs](#)

add_assessment_datasource

This command adds a datasource to a security assessment.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/assessment_datasource
```

GuardAPI syntax

```
add_assessment_datasource parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|--|
| assessmentDescription | String | Required. This string is a variable that is unique. Ensure that there is no previous assessment with the same description. If there is an existing one, an error occurs. |
| datasourceName | String | Required. This string is a variable, and must be the name of an existing data source. If a datasource with the defined string is not present, then an error occurs. |

Example

```
grdapapi add_assessment_datasource assessmentDescription=Assess1 datasourceName=DS1
```

add_assessment_datasource_group

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/assessment_datasource_group
```

GuardAPI syntax

```
add_assessment_datasource_group parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|-------------|
| assessmentDescription | String | Required. |
| groupName | String | Required. |

add_assessment_test

This command adds a test to an existing security assessment.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/assessment_test
```

GuardAPI syntax

```
add_assessment_test parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|--|
| assessmentDescription | String | Required. |
| datasourceType | String | For valid values, call add_assessment_test from the command line with --help=true. |
| exceptionsGroup | String | |

| Parameter | Value type | Description |
|-----------------|------------|--|
| explanation | String | |
| fromDate | String | |
| severity | String | Valid values: <ul style="list-style-type: none">• <i>Critical</i>• <i>Major</i>• <i>Minor</i>• <i>Caution</i>• <i>Info</i> |
| testDescription | String | Required. |
| testseparator | String | The testseparator parameter specifies the delimiter that is used to separate tests when multiple test descriptions are included in the command. This parameter provides clarity when an individual testDescription also contains delimiters such as a comma. The GuardAPI uses the delimiter specified in the testseparator parameter to identify each test when the command is parsed. As an example, if a test description contains a comma, and multiple tests are separated by a semicolon, specify ';' as the testseparator.

Valid values: <ul style="list-style-type: none">• ,• ;• ^• ~• \\
• * The default value is ";". |
| threshold | String | |
| toDate | String | |

Example

```
grdapi add_assessment_test assessmentDescription="!DPS 2020 Q1 Testing - 2014 (MS SQL) EDS New Tests"
testDescription="Description 1 SQL Server must be configurable to overwrite audit log records, oldest first, in the event of
unavailability of space for more audit log records; Description 2 Another valid test description" testseparator=";"
```

This example adds the tests "Description 1 SQL Server must be configurable to overwrite audit log records, oldest first, in the event of unavailability of space for more audit log records" and "Description 2 Another valid test description" to the assessment "!DPS 2020 Q1 Testing - 2014 (MS SQL) EDS New Tests". The testseparator parameter specifies that the delimiter ";" is used to separate multiple tests in the command.

add_assessment_test_by_dsid

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/assessment_test
```

GuardAPI syntax

```
add_assessment_test_by_dsid parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|--|
| assessmentDescription | String | Required. |
| dataSourceType | String | For valid values, call add_assessment_test_by_dsid from the command line with <code>--help=true</code> . |
| exceptionsGroup | String | |
| explanation | String | |
| fromDate | String | |
| severity | String | Valid values: <ul style="list-style-type: none">• <i>Critical</i>• <i>Major</i>• <i>Minor</i>• <i>Caution</i>• <i>Info</i> |
| threshold | String | |
| toDate | String | |

add_autodetect_task

Use this command to add an auto-discovery process to the specified host and port name(s).

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/add_autodetect_task
```

GuardAPI syntax

```
add_autodetect_task parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| hosts_list | String | Required. Lists of hosts. Space separated list of IPs or IP ranges and wild cards such as 192.168.0.1 192.168.1.* |
| ports_list | String | Required. Comma separated list of ports or port ranges, such as: 22,23,1400-1600. |
| process_name | String | Required. Name of the auto-discovery process |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To add the auto-discovery task myProcess to the hosts 192.168.1.1 and 192.168.1.3, on ports 22 and 23:

```
grdap api add_autodetect_task process_name=myProcess hosts_list="192.168.1.1 192.168.1.3" ports_list="22,23"
```

Related concepts

- [Database auto-discovery](#)

Related reference

- [Auto-discovery APIs](#)

add_available_test_notes

Add custom descriptions to vulnerability assessment test results. As an example, add a custom risk score for your test to a user-defined field. Then, use the Query-Report builder to add the custom field to your custom report. You can then view the custom risk score when you generate the custom report.

This API is available in Guardium v11.5 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/available_test_notes
```

GuardAPI syntax

```
add_available_test_notes parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| | | |

| Parameter | Value type | Description |
|-------------------------|------------|---|
| datasourceType | String | Required. For valid values, call add_available_test_notes from the command line with --help=true. |
| override | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| testDescription | String | Required. |
| userDefinedNotes | String | Custom comment. |
| userDefinedReferenceOne | String | Custom comment. |
| userDefinedReferenceTwo | String | Custom comment. |

Example

The following example adds custom_notes and custom_reference_text to va_test:

```
grdapi add_available_test_notes testDescription="va_test" datasourceType="MS SQL SERVER" userDefinedNotes="custom_notes"
userDefinedReferenceOne="custom_reference_text"
```

add_classifier_datasource

This command adds classification datasources.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/classifier_datasource
```

GuardAPI syntax

```
add_classifier_datasource parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|-------------|
| datasourceName | String | Required. |
| processName | String | Required. |

add_classifier_datasource_group

This command adds classification datasource groups.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/classifier_datasource_group
```

GuardAPI syntax

```
add_classifier_datasource_group parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|-------------|
| groupName | String | Required. |
| processName | String | Required. |

add_cluster

Use this API to add a new S-TAP cluster or make changes to an existing S-TAP cluster.

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/add_cluster
```

GuardAPI syntax

```
add_cluster parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------|------------|---|
| clusterName | String | Required. |
| connectivity | Boolean | Required. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| desc | String | |
| memberList | String | |
| traffic | Boolean | Required. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| virtualIp | String | |

add_connection_properties

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/con_properties
```

GuardAPI syntax

```
add_connection_properties parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| fullReplace | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| name | String | Required. |
| properties | String | Required. |
| type | String | Required. For valid values, call add_connection_properties from the command line with <code>--help=true</code> . |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

add_custom_property_to_datasource_by_id

This command adds a custom property to a datasource that is identified by its identification key.

This API is available in Guardium V11.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/datasource_custom_prop_add
```

GuardAPI syntax

```
add_custom_property_to_datasource_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| customProps | String | Required. |
| id | Integer | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related concepts

- [Datasource APIs](#)

add_custom_property_to_datasource_by_name

This command adds a custom property to a datasource that is identified by its name.

This API is available in Guardium V11.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/datasource_custom_prop_add
```

GuardAPI syntax

```
add_custom_property_to_datasource_by_name parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|-------------|
| customProps | String | Required. |
| name | String | Required. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related concepts

- [Datasource APIs](#)

add_custom_property_to_datasources_in_group

This API is available in Guardium V11.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/datasource_group_custom_prop_add
```

GuardAPI syntax

```
add_custom_property_to_datasources_in_group parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| customProps | String | Required. |
| name | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

add_datasource_to_entitlement_optimization

Adds the data from this datasource to the entitlement optimization data collection, and generates details to the individual entitlement optimization tabs as specified.

This API is available in Guardium V10.1.4 and later.

Use the following table to determine which data to extract for each feature:

Table 1. enable_entitlement_optimization parameters required per analysis type

| | What's New
(generateNews) | Users and
Roles | Recommendations
(generateRecommendations) | Browse
Entitlements | What If
(generateRoleClusters) |
|--------------------|------------------------------|--------------------|--|------------------------|-----------------------------------|
| extractActivity | | | | X | X |
| extractEntitlement | X | X | X | X | |

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

PUT https://[Guardium hostname or IP address]:8443/restAPI/addDataSourceToEntitlementOptimization

GuardAPI syntax

`add_datasource_to_entitlement_optimization parameter=value`

Parameters

| Parameter | Value type | Description |
|-------------------------|------------|---|
| datasourceName | String | Required. Guardium datasource name. |
| extractActivity | Boolean | Required. Datasource is enabled or disabled for entitlement optimization. Set to true to generate data in the Browse Entitlements and What If? tabs. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 |
| extractEntitlement | Boolean | Enables or disables extraction of entitlement data. Set to true to generate data in the What's New?, Users and Roles, Recommendations, and Browse Entitlements tabs. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 |
| filterIgnoreVerbs | Boolean | For future use. Ignore verbs are filtered from the data source's collected data. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 |
| filterTempObjects | Boolean | For future use. Temporary objects are filtered from the data source's collected data. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 |
| generateNews | Boolean | Activity from this datasource is included in the What's New tab. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 |
| generateRecommendations | Boolean | Activity from this datasource is included in the Recommendations tab. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 |
| generateRoleClusters | Boolean | Enables or disables extraction of behavioral role clustering from the data source, used in the What If tab. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Set to true to generate data in the What If? tab.
Default = 0 |
| isEnabled | Boolean | Required. Datasource is enabled / disabled, for entitlement optimization. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 |
| objectScope | String | Entitlement recommendations show results only for this specified object groups.
Valid values: One or more comma separated Guardium object group IDs (groups must contain only objects).
default = NULL |
| userScope | String | Entitlement recommendations show results only for the specified user groups (groups must contain only users).
default = NULL |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Enable entitlement optimization and generate data for the What's New? tab for data from the datasource SSQLSERVER.

```
grdapi add_datasource_to_entitlement_optimization datasourceName=SSQLSERVER isEnabled=1 generateNews=1
```

Enable entitlement optimization and generate data for the What's New? and Browse Entitlements tabs for data from the datasource SSQLSERVER.

```
grdapi add_datasource_to_entitlement_optimization datasourceName=SSQLSERVER isEnabled=1 generateNews=1 extractEntitlement=1 extractActivity=1
```

Adds data from this datasource to the Recommendations tab, filtered for the users in usergroup123 only.

```
grdapi add_datasource_to_entitlement_optimization datasourceName=SSQLSERVER extractEntitlement=1 generateRecommendations=1 userScope=usergroup123
```

Related concepts

- [Entitlement optimization](#)

Related reference

- [Entitlement optimization APIs](#)

add_datasource_to_group

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/datasource_group_add
```

GuardAPI syntax

```
add_datasource_to_group parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|-------------|
| datasourceName | String | Required. |
| groupName | String | Required. |

add_dm_to_profile

A profile is a group of data marts that are activated together. Use this command to create a profile from scratch.

This API is available in Guardium V10.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/datamartInProfile
```

GuardAPI syntax

```
add_dm_to_profile parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| category | String | Informational. |
| cron_string | String | The schedule setting for the datamart. Omit this parameter to use the default. It's recommended to use the default, which takes into account all the schedules of Guardium's automatic processes. If you are adding a user-defined DM, there is no default cron_string. |
| datamart_name | String | Required. Adds this datamart to the profile. For valid values, call add_dm_to_profile from the command line with --help=true. |
| profile_name | String | Required. The datamart is added to this profile. For valid values, call add_dm_to_profile from the command line with --help=true. |
| unit_type | String | The type of Guardium® system. Valid values: <ul style="list-style-type: none">• ANY• CM• CM/STANDALONE• AGGREGATOR• COLLECTOR• STANDALONE |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Example

To add the data mart `Export:Full SQL` to the user defined profile `sql_all`.

```
add_dm_to_profile profile_name=sql_all datamart_name=Export:Full SQL
```

Related concepts

- [Data Mart](#)

Related reference

- [Data mart APIs](#)

add_domain_to_universal_connector_allowed_domains

Run this API to authorize communication with cloud-based database domains.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/addDomainToUcAllowedDomains
```

GuardAPI syntax

```
add_domain_to_universal_connector_allowed_domains parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| domain | String | Required. Cloud-based domain name to add. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To authorize communication with AWS APIs:

```
grdapi add_domain_to_universal_connector_allowed_domains domain=amazonaws.com
```

Related reference

- [Guardium universal connector APIs](#)

add_group_to_quick_search

This command adds groups to the quick search facet drop-down menus, so that you can select the groups for filtering the investigation dashboard results.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
add_group_to_quick_search parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------|------------|---|
| facet | String | <p>Required. The facet of the group you are adding. Valid values:</p> <ul style="list-style-type: none"> • DB_USER • OS_USER • OBJECT • VERB • FAM_COMMAND • SERVER_IP |
| group_description | String | Required. Group name you are adding, of the specified facet type. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To add server_group5 to the quick search:

```
add_group_to_quick_search facet=SERVER_IP group_description=server_group5
```

Related concepts

- [Investigation dashboard](#)

Related reference

- [Investigation dashboard APIs](#)

add_ip_to_sg

This API adds the specified Guardium® IP to a cloud security group.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/add_ip_to_sg
```

GuardAPI syntax

```
add_ip_to_sg parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| datasource_name | String | Required. A cloud datasource defined in Guardium. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related tasks

- [Cloud database service protection with native audit](#)

Related reference

- [Native audit APIs](#)

add_mfa_exempt_users

Use this command to enter a list of users who are exempt from secondary authentication for multi-factor authentication.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/configure_mfa
```

GuardAPI syntax

```
add_mfa_exempt_users parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|---|
| exemptUsers | String | A comma-separated list of one or more users to exempt from multi-factor authentication. |
| mfaType | String | Required. The authentication type. For valid values, call <code>add_mfa_exempt_users</code> from the command line with <code>--help=true</code> . |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GaurdAPI example

```
grdapi add_mfa_exempt_users exemptUsers="Hadrian,Fred,admin" mfaType=DUO
```

Related concepts

- [Portal configuration](#)

Related reference

- [remove_mfa_exempt_users](#)

add_objects_native_audit

This API adds objects to the object audit (audit trail) on the specified datasource.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/add_objects_native_audit
```

GuardAPI syntax

```
add_objects_native_audit parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| datasource_name | String | Required. A cloud datasource defined in Guardium. |
| objects | String | Required. Comma-separated list of objects. View objects with the <code>get_native_audit_objects</code> API or in the GUI. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related tasks

- [Cloud database service protection with native audit](#)

Related reference

- [Native audit APIs](#)

[add_ranger_config](#)

Use this command to define a Ranger on an Ambari server for Hadoop monitoring.

This command requires valid administrative authority on the Ambari server such as an admin or service administrator account. The Ambari administrator must restart the affected Hadoop components, so that the changes take effect.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/add_ranger_config
```

GuardAPI syntax

```
add_ranger_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| clusterName | String | Required. Ambari cluster name. |
| hostname | String | Required. Hostname or IP address of the Ambari server. |
| password | String | Required. Password for the admin user specified by <code>userName</code> |
| port | Integer | Port on the Ambari server for the user interface. Default = 8080. |
| sslEnabled | Boolean | Sets whether SSL is enabled for communication with this Ranger. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| userName | String | Required. Ambari server username; must be an admin or service admin user. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GrdAPI Example

To define a ranger cluster

```
grdapic add_ranger_config hostname=hw-cl4-05 userName=admin port=8080 password=xxxxxx clusterName=Cluster4
```

Sample output:

```
ID=0Configuration for Cluster: Cluster4 added.
```

REST API example

```
curl -k --header "Authorization:Bearer <access token>" -i -H "Content-Type: application/json" -X POST -d '{hostname="hw-cl4-05", userName="admin", port=8080, password="admin", clusterName="Cluster4"}' https://<Guardium server name>:8443/restAPI/add_ranger_config
```

Sample output:

```
[{"id": 2, "clusterName": "Cluster4", "serverHost": "hw-cl4-05", "serverPort": 8080, "userName": "admin", "lastRefresh": "2016-09-27 11:31:03", "status": []}]
```

Related concepts

- [Hadoop integration using Hortonworks and Apache Ranger](#)

Related reference

- [Hadoop monitoring APIs](#)
- [S-TAP Hadoop parameters](#)

add_ranger_hdfs_config

Use this command to add a Hadoop integration with Ranger HDFS.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/add_ranger_hdfs_config
```

GuardAPI syntax

```
add_ranger_hdfs_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------------------|------------|---|
| ldLibraryPath | String | Locate libjvm.so (for example, /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.191.b12-1.el7_6.x86_64/jre/lib/amd64/server/libjvm.so) and set <code>ld_library_paths</code> to the directory that contains libjvm.so (for example, /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.191.b12-1.el7_6.x86_64/jre/lib/amd64/server). |
| principal | String | Required for Kerberos. The value of Ranger HDFS user. |
| rangerHdfsAuditDirs | String | Comma-separated list of directories where Ranger logs the service audits. Include one directory that contains the daily log directories, for each service you want to monitor. Usually the paths are located under /ranger/audit.

Example service directories for CDP 7: /ranger/audit/hive/hiveServer2,/ranger/audit/kafka/kafka,/ranger/audit/hbase/hbaseMaster,/ranger/audit/hbase/hbaseRegional,/ranger/audit/atlas/atlas,/ranger/audit/hdfs/hdfs

Example service directories for HW 3: /ranger/audit/hbaseMaster,/ranger/audit/hbaseRegional,/ranger/audit/hdfs,/ranger/audit/hiveServer2,/ranger/audit/kafka,/ranger/audit/solr,/ranger/audit/storm |
| rangerHDFSAuditHistoryLength | Integer | Required. |
| rangerHdfsKeytab | String | Required for Kerberos. Location of the Kerberos keytab that contains the principal used to connect to HDFS. |
| rangerHdfsLibLocation | String | Locate libhdfs.so provided by Hadoop cluster (for example, /usr/hdp/3.1.0.141-1/usr/lib/libhdfs.so) and set <code>ranger_hdfs_lib_location</code> to the directory that contains libhdfs.so (for example, /usr/hdp/3.1.0.141-1/usr/lib). |
| rangerHdfsNameNode | String | IP or hostname of the HDFS NameNode. |
| rangerHdfsPollMs | Integer | Time interval, in milliseconds, the S-TAP® waits between checking for new Ranger audits in HDFS. |
| rangerHdfsPort | Integer | The HDFS NameNode port the S-TAP connects to. |
| rangerHdfsUser | String | The user with which S-TAP connects to HDFS. If the HDFS setup is using Kerberos, set the parameter to the Kerberos principal. |
| stapHostName | String | Required. Host name or IP of the S-TAP that receives the Ranger audit messages from the Ranger. |
| useKerberos | Boolean | Enables Kerberos authentication for this connection. When enabled, requires values for Principal and Ranger HDFS keytab. Valid values: <ul style="list-style-type: none">• 0: Disabled• 1: Enabled Default = 0 |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Related concepts

- [Hadoop integration using Ranger HDFS for Hortonworks and Cloudera 7](#)

Related reference

- [Hadoop monitoring APIs](#)
- [S-TAP Hadoop parameters](#)

add_ranger_service

Use this command to map the Ranger service to an S-TAP®, using the S-TAP host and port from the output to `get_ranger_staps`.

This command requires valid administrative authority on the Ambari server such as an admin or service administrator account. After running the command, the Ambari administrator must restart the affected Hadoop components so that the changes take effect.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/add_ranger_service
```

GuardAPI syntax

```
add_ranger_service parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|---|
| clusterName | String | Required. Ambari cluster name defined with <code>add_ranger_config</code> . |
| enableMonitoring | Boolean | Required. Enable Guardium® monitoring for this Hadoop service. Valid values: <ul style="list-style-type: none">• 0: false• 1: true Default = 0 |
| port | Integer | Port on the Ambari server for listening. Default = 5555. |
| serviceName | String | Required. Name of the service. Valid values: <ul style="list-style-type: none">• hdfs• hive• hbase• kafka• solr• storm |
| stapHostName | String | Required. Host name or IP of the S-TAP that receives the log4j audit messages from the Ranger. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GrdAPI example

To add a Ranger service on Cluster4, listening port on the Ambari server of 5555, and S-TAP host <db server>:

```
grdapic add_ranger_service clusterName=Cluster4 serviceName=HDFS stapHostName=<db server> port=5555 enableMonitoring=true
```

System response:

ID=0

The Hadoop service configuration has been changed. Ask the Hadoop administrator to restart the Hadoop service to activate the change.
HDFS Monitoring Enabled on <db server>:5565

REST API example

This example specifies DFS, HIVE, and HBASE:

```
curl -k --header "Authorization:Bearer <access token>" -i -H "Content-Type: application/json" -X POST -d
'{clusterName="Cluster4", serviceName="HDFS,HIVE,HBASE", stapHostName="<db server>", port=5534, enableMonitoring=true}'
```

Sample output:

```
[  
  {  
    "id": 3,  
    "ambariConfigId": 1,  
    "service": {  
      "id": 1,  
      "label": "HBase",  
      "value": "HBASE"  
    },  
    "stapHost": {  
      "id": 18,  
      "name": "<db server>",  
      "value": "<db server>",  
      "port": "5534",  
      "stapStatus": 2  
    },  
    "isMonitored": true,  
    "port": "5534",  
    "editMode": true  
  },  
  {  
    "id": 1,  
    "ambariConfigId": 1,  
    "service": {  
      "id": 2,  
      "label": "HDFS",  
      "value": "HDFS"  
    },  
    "stapHost": {  
      "id": 18,  
      "name": "<db server>",  
      "value": "<db server>",  
      "port": "5534", "stapStatus": 2  
    },  
    "isMonitored": true,  
    "port": "5534",  
    "editMode": true  
  },  
  {  
    "id": 2,  
    "ambariConfigId": 1,  
    "service": {  
      "id": 3,  
      "label": "Hive",  
      "value": "HIVE"  
    },  
    "stapHost": {  
      "id": 18,  
      "name": "<db server>",  
      "value": "<db server>",  
      "port": "5534",  
      "stapStatus": 2  
    },  
    "isMonitored": true,  
    "port": "5534",  
    "editMode": true  
  }  
]
```

Related concepts

- [Hadoop integration using Hortonworks and Apache Ranger](#)

Related reference

- [Hadoop monitoring APIs](#)
- [S-TAP Hadoop parameters](#)

add_receiver_to_rule_action

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/receiver_to_rule_action
```

GuardAPI syntax

```
add_receiver_to_rule_action parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------------|------------|---|
| actionName | String | Required. |
| alertUserLoginName | String | |
| classDestination | String | |
| fromPolicy | String | Required. |
| notificationType | String | Required. |
| ruleDesc | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

add_stream

This command adds a data stream for cloud database service protection. After you define a Guardium cloud DB service account, you can discover or define available data streams and assign them to Guardium collectors.

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/datasream
```

GuardAPI syntax

```
add_stream parameter=value
```

Amazon-specific parameters

| Parameter | Value type | Description |
|---------------------|------------|---|
| activate | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true): Start the data stream. Default = 0 (false) |
| cloudTitle | String | Required. The name of the cloud DB service account. For valid values, call add_stream from the command line with <code>--help=true</code> . For more information, see Define, modify, and delete AWS DB service accounts . |
| cluster_resource_id | String | Required. The cluster resource ID for the AWS RDS cluster associated with the stream. |
| collectorHostNames | String | Required. The names of your Guardium collectors, for example: <code>collector01.yourcompany.com</code> For valid values, call add_stream from the command line with <code>--help=true</code> . |
| consumerGroupName | String | Required. The consumer group name that you assign from the Guardium® Cloud DB Service Protection page. For more information, see Discover and configure AWS data streams . |
| db_DNS_endpoint | String | Required. The DB DNS endpoint. |
| dbType | String | The database for this stream. Valid values: <ul style="list-style-type: none">• AuroraMySQL - Datastreams only• AuroraPostgreSQL - Datastreams only• Oracle - Native audit only Default = <code>AuroraPostgreSQL</code> |
| port | String | Required. The DB DNS endpoint port. |

| Parameter | Value type | Description |
|------------|------------|---|
| region | String | Required. For valid values, call add_stream from the command line with --help=true. |
| streamName | String | Required. The name of the stream from the RDS cluster configuration. |

| | | |
|-----------------|--------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |
|-----------------|--------|---|

Azure-specific parameters

| Parameter | Value type | Description |
|-------------------------|------------|---|
| activate | Boolean | <p>Activates data streaming. Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true): Start the data stream <p>Default = 0 (false)</p> |
| cloudTitle | String | Required. The name of the cloud DB service account. For more information, see Define, modify, and delete Azure cloud database service accounts . |
| collectorHostNames | String | Required. The names of your Guardium collectors, for example: <code>collector01.yourcompany.com</code> . For valid values, call add_stream from the command line with --help=true. |
| consumerGroupName | String | Required. The Azure consumer group name. |
| db_DNS_endpoint | String | Required. The DB DNS endpoint. |
| dbType | String | <p>The database for this event hub stream. Valid values:</p> <ul style="list-style-type: none"> • AzureSQL • CosmosSQL • CosmosMongoDB • CosmosCassandra • CosmosGremlin • CosmosTable <p>Default = AzureSQL</p> |
| namespace | String | The Azure event hub namespace. |
| port | String | Required. The DB DNS endpoint port. |
| storageConnectionString | String | The Azure storage connection string name |
| streamName | String | Required. The event hub name. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related tasks

- [Define, modify, and delete AWS cloud DB service accounts](#)
- [Define, modify, and delete Azure cloud database service accounts](#)

add_threshold_to_rule

You can use your policies' rules to create active threat analytics case types, by setting a threshold on specific violation policy rules that have a severity of high in the rule definition, and the rule action is **Alert per match**.

When the rule threshold is exceeded in any 1 hour, a case is created. The case type is the name of the rule. Cases that are created from a policy rule threshold appear in the active threat analytics cases table, and are treated like any other case.

Changes to installed policies are applied according to the policy schedule. When adding a threshold to a rule in an installed policy, cases are created for violations (according to the threshold) only after the policy is reinstalled.

You cannot define thresholds in the GUI.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/add_threshold_to_rule
```

GuardAPI syntax

```
add_threshold_to_rule parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| policy_name | String | The policy that has the rule you want to add a threshold to. Use the API <code>list_policy</code> to view policies. |
| rule_name | String | The rule you want to add a threshold to. Use the API <code>list_policy_rules</code> to view rules. |
| threshold_value | Integer | The threshold at which a case is created. |

Examples

To add the threshold 25 to ruleNNN in policyAAA:

```
grdapi add_threshold_to_rule policy_name=policyAAA rule_name=ruleNNN threshold=25
```

Related tasks

- [Creating threat categories from policy rules](#)

Related reference

- [Policy and rule APIs](#)
- [Active threat analytics and risk spotter APIs](#)
- [list_policy_rules](#)
- [list_policy](#)

add_time_period

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/time_period
```

GuardAPI syntax

```
add_time_period parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|--|
| contiguous | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| hourFrom | String | Required. |
| hourTo | String | Required. |
| timePeriodDescription | String | Required. |
| weekdayFrom | String | Required. |
| weekdayTo | String | Required. |

aggregation

12.1 and later This API command is used to archive the data and export it.

REST API syntax

This API is available as a REST service with the `aggOnDemandApi` method. Call this API as follows:

```
https://[Guardium hostname or IP address]:8443/restAPI/agg_onDemand
```

GuardAPI syntax

```
aggregation parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| from | String | The from parameter should be less than to parameter, and should be earlier than the current date. |
| to | String | The to parameter should be earlier than the current date. |
| type | String | Valid values: <ul style="list-style-type: none">• <code>export</code>• <code>archive</code> |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

The following command runs the export job.

```
grdapi aggregation type=export from=2024-01-01 to=2024-01-02  
ID=0  
Executing export using default interval
```

The following command runs the archive job.

```
grdapi aggregation type=archive from=2023-12-20 to=2024-01-02  
ID=0
```

The following command runs the archive job. If no from and to dates are provided, the default settings are used.

```
grdapi aggregation type=archive  
ID=0  
Executing archive job
```

apply_rules_on_discoveredinstances

This API pulls information that is defined in the Database Discovered Instances Rules UI and immediately applies the rules to the S-TAPs on the primary collectors. Run `apply_rules_on_discoveredinstances` only on Guardium managed units or stand-alone systems.

For more information about discovered instances rules, see [Database discovered instances rules](#).

This API is available in Guardium V10.6 and V11.1 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/applyRules
```

GuardAPI syntax

```
apply_rules_on_discoveredinstances parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
>grdapi apply_rules_on_discoveredinstances api_target_host=10.0.1.123
>grdapi apply_rules_on_discoveredinstances debug=2

Sample output

ID=0
Global rules are enabled.
Collector rules are enabled.
Number of discovered instances: 9
Processed timestamp: 2022-05-03 06:49:24.0
Updated timestamp: Tue May 03 17:59:40 EDT 2022

Warnings: []0.0.234.157=
    addedEngines=[]
    discoveredInstances=[b91c2e6854c67370f32f72a6c7c9fe844d15652a, 79cbfb016426dd4cbce50aa2c57a3468c7e1d185,
ca9bfe29dc02d136648b229828f40333e839e93]
    excludedEngines=[]
    excludedInstances=[]
    filteredInstances=[b91c2e6854c67370f32f72a6c7c9fe844d15652a]
    ignoredEngines=[oracle_0.0.234.157(1521,1521,DB_1), oracle_0.0.234.157(1521,1521,DB_2)]
    messages=[]
    replacedEngines=[]

0.0.234.158=
    addedEngines=[]
    discoveredInstances=[e6f108f9a197db3040aa3647093605a8da12345, 4cb7c413c01c615abdb249bb2231ec54c8612345,
4ef2ec20cf2449cc9876ba417a65a2ba1a12345]
    excludedEngines=[]
    excludedInstances=[]
    filteredInstances=[4ef2ec20cf2449cc9876ba417a65a2ba1a12345]
    ignoredEngines=[oracle_0.0.234.158(1521,1521,DB_0), oracle_0.0.234.158(1521,1521,DB_1)]
    messages=[]
    replacedEngines=[]
...
```

Related concepts

- [Database discovered instances rules](#)

Related information

- [Inspection engine parameters](#)

assign_analytic_case

Use this command to assign a threat analytics or risk spotter case to a Guardium email, group, role, or user.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/analytic_case
```

GuardAPI syntax

```
assign_analytic_case parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------------|------------|---|
| case_id | Long | Required for Advanced threat analytics only. The case ID is in the Case # column in the GUI. |
| DBUser | String | Required for Risk Spotter only. The DB user associated with the risk, as seen in the GUI. |
| emails | String | Required if receiver_type=email. Comma separated list of email addresses. |
| email_content_type | Integer | Required if receiver_type=email. <ul style="list-style-type: none">• 0: PDF• 1: CSV Default = 0 |
| isRiskSpotter | Boolean | Required for Risk Spotter only. Identifies the case as a RiskSpotter case. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| iterationID | Integer | Risk Spotter only. Indicates if this case is a Risk spotter case only. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| receiver | String | Required if receiver_type = one of group, role, or user. Valid values: <ul style="list-style-type: none">• For group: valid Guardium user group that has at least one member• For role: valid Guardium role that has at least one member• For user: valid Guardium user |
| receiver_type | Integer | Required. Determines who the ticket is assigned to. Valid values: <ul style="list-style-type: none">• 1: email• 2: role• 3: group• 4: user |
| serverIP | String | Required for Risk Spotter only. Server IP associated with the risk, as seen in the GUI. |

Examples

To assign the advanced threat analytics case 145 to the guardium group "group24":

```
grdapi assign_analytic_case case_id=145 receiver_type=3 receiver=group24
```

assign_collectors

This API assigns Guardium collectors for cloud-based service accounts in central manager configurations.

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/datasream
```

GuardAPI syntax

```
assign_collectors parameter=value
```

Amazon-specific parameters

| Parameter | Value type | Description |
|------------|------------|---|
| activate | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true): Start the data stream. Default = 0 (false) |
| cloudTitle | String | Required. The name of the cloud DB service account. For valid values, call assign_collectors from the command line with --help=true
For more information, see Define, modify, and delete AWS DB service accounts . |

| Parameter | Value type | Description |
|---------------------|------------|---|
| cluster_resource_id | String | Required. The cluster resource ID for the AWS RDS cluster associated with the stream. |
| collectorHostNames | String | Required. The names of your Guardium collectors, for example: <code>collector01.yourcompany.com</code> . For valid values, call <code>assign_collectors</code> from the command line with <code>--help=true</code> . |
| consumerGroupName | String | Required. The consumer group name that you assign from the Guardium® Cloud DB Service Protection page. For more information, see Discover and configure AWS data streams . |
| db_DNS_endpoint | String | Required. The DB DNS endpoint. |
| port | String | Required. The DB DNS endpoint port. |
| region | String | Required. For valid values, call <code>assign_collectors</code> from the command line with <code>--help=true</code> . |
| streamName | String | Required. The name of the stream from the RDS cluster configuration. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • <code>all_managed</code>: execute on all managed units but not the central manager • <code>all</code>: execute on all managed units and the central manager • <code>group:<group_name></code>: execute on all managed units identified by <code><group name></code> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Azure-specific parameters

| Parameter | Value type | Description |
|-------------------------|------------|---|
| activate | Boolean | <p>Activates data streaming. Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true): Start the data stream <p>Default = 0 (false)</p> |
| cloudTitle | String | Required. The name of the cloud DB service account. For valid values, call <code>assign_collectors</code> from the command line with <code>--help=true</code> . For more information, see Define, modify, and delete Azure cloud database service accounts . |
| collectorHostNames | String | The names of your Guardium collectors, for example: <code>collector01.yourcompany.com</code> . For valid values, call <code>assign_collectors</code> from the command line with <code>--help=true</code> . |
| consumerGroupName | String | The Azure consumer group name. |
| db_DNS_endpoint | String | Required. The DB DNS endpoint. |
| namespace | String | The Azure event hub namespace. |
| port | String | Required. The DB DNS endpoint port. |
| storageConnectionString | String | The Azure storage connection string name |
| streamName | String | Required. The event hub name. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • <code>all_managed</code>: execute on all managed units but not the central manager • <code>all</code>: execute on all managed units and the central manager • <code>group:<group_name></code>: execute on all managed units identified by <code><group name></code> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related tasks

- [Define, modify, and delete AWS cloud DB service accounts](#)
- [Define, modify, and delete Azure cloud database service accounts](#)

assign_load_balancer_groups

This command assigns a managed unit group to an application or S-TAP® group to help manage load balancing requirements.

Use this command to assign a specific S-TAP group to one or more load balance-enabled managed unit groups. When S-TAP needs to failover to a new managed unit, Guardium allocates a managed unit from one of the assigned load balancer (failover) groups.

Use failoverGroupPriority to assign specific priority to S-TAP or managed unit groups. If you do not assign a priority, Guardium randomly assigns the failover managed unit when required.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
assign_load_balancer_groups parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|--|
| appGroupName | String | Required. The application or S-TAP group name. |
| isFailoverGroup | Boolean | If set to 1, this managed unit group is a member of a failover group. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| failoverGroupPriority | String | Required when isFailoverGroup = 1 (true) and one or more S-TAP groups already have assigned priorities. Must be an integer value.
If not specified, the priority is 1. |
| muGroupName | String | Required. The managed unit group name. |

Related concepts

- [Using the group builder](#)

Related tasks

- [Creating managed unit groups](#)

assign_qr_condition_to_action

This command creates an association between a query rewrite condition and an associated action.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/qr_condition_to_action
```

GuardAPI syntax

```
assign_qr_condition_to_action parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|--|
| actionName | String | Required. The name of the query rewrite action. |
| conditionName | String | Required. The name of the query rewrite condition to be associated with the specified action. |
| definitionName | String | Required. The name of the query rewrite definition that is associated with the specified condition and action. |

Examples

To associate the condition "qr cond15_2" with the action "qr action15_2", and give it the definition name "case 15":

```
grdapi assign_qr_condition_to_action definitionName="case 15" actionName="qr action15_2" conditionName="qr cond15_2"
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

audit_process_run_status

Displays the run status for a specified audit process.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/audit_process_run_status
```

GuardAPI syntax

```
audit_process_run_status parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|--|
| processName | String | Required. The name of an audit process. Use list_audit_processes to find the audit process name. |

Related concepts

- [Building audit processes](#)

auto_execute_suggested_dependencies

This command enables job dependencies for the specified task.

This command is equivalent to selecting the option Auto run dependent jobs in the Scheduler of a task. Guardium automatically finds all the job's prerequisite jobs and runs them in order, before running this job. This ensures that the job runs with the latest, most accurate data.

This API is available in Guardium V10.1.4 and later.

GuardAPI syntax

```
auto_execute_suggested_dependencies parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| jobTrigger | String | Required. The name of the task whose dependent tasks you want to run. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • <code>all_managed</code>: execute on all managed units but not the central manager • <code>all</code>: execute on all managed units and the central manager • <code>group:<group name></code>: execute on all managed units identified by <code><group name></code> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To enable the job dependencies for the job userSynchronizationTrigger:

```
grdapi auto_execute_suggested_dependencies jobTrigger=userSynchronizationTrigger
ID=0
ok
```

Related concepts

- [Scheduling](#)
- [Job dependencies](#)

Related reference

- [Schedule and job dependencies APIs](#)
-

backup_cm_list_candidates

Use this command, on a central manager only, to identify the possible backup, or secondary, central managers from among the registered units in the environment.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/backup_cm_list_candidates
```

GuardAPI syntax

```
backup_cm_list_candidates
```

This API takes no parameters.

GrdAPI example

To list IPs of potential secondary central managers, enter:

```
grdapi backup_cm_list_candidates
```

Format of output:

```
<ip> (<hostname>)
<ip> (<hostname>)
<ip>
```

REST API example

To list IPs of potential secondary central managers, enter:

```
curl \
-k --header "Authorization:Bearer d51c41d0-a6b1-4aa3-90bc-5232a44e8b0d" \
--include --header "Content-Type: application/json" \
-X GET https://localhost:8443/restAPI/backup_cm_list_candidates
```

Format of output:

```
<ip> (<hostname>)
<ip> (<hostname>)
<ip>
```

Related concepts

- [Central manager redundancy](#)
-

backup_cm_set

Use this command, on a central manager only, to define a backup, or secondary, central manager.

This API is available in Guardium V11.2 and later.

Note: Switching to a backup central manager interrupts communication with collectors and may generate the following message: "Central manager experienced failed data transfer from collector." The issue is visible in the Scheduled Jobs Exceptions report and should clear within 24-hours.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/backup_cm
```

GuardAPI syntax

```
backup_cm_set parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| ip | String | Required. The IP of the backup central manager. For valid values, call <code>backup_cm_set</code> from the command line with <code>--help=true</code> . Enter this parameter with no IP value to delete the current secondary central manager. |

GuardAPI example

To set the backup central manager to 9.142.10.100, enter this command on the primary central manager:

```
grdapi backup_cm_set ip=9.142.10.100
Backup CM designated
```

Output if the IP is invalid or not one of the allowed candidates:

```
Wrong value: "ip" must be one of
<ip> (<hostname>)
<ip> (<hostname>)
<ip>
...
ERR=23
Value not in constant list.
```

REST API example

To set the backup central manager to 9.142.10.100:

```
curl \
-k --header "Authorization: Bearer d51c41d0-a6b1-4aa3-90bc-5232a44e8b0d" \
--include --header "Content-Type: application/json" \
-X PUT --data '{"ip":"9.142.10.100"}' https://<CM-hostname>:8443/restAPI/backup_cm
```

Related concepts

- [Central manager redundancy](#)

Related reference

- [Central management APIs](#)

cancel_distributed_report_target

Use this API to remove a Guardium system from the list of distributed report targets.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
cancel_distributed_report_target parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|--|
| target_host_name | String | Required. IP or hostname of the Guardium system. |

Examples

To remove the Guardium system with the IP 11.11.11.11 from the list of targets for distributed reports:

```
grdapi cancel_distributed_report_target target_host_name=11.11.11.11
```

Related concepts

- [Distributed report builder](#)

Related reference

- [Reports and report generation APIs](#)

change_cli_password

The command changes the password for the cli user.

The minimum password length (8 or 15) depends on the [enable_strong_cli_password](#) setting.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/change_cli_password
```

GuardAPI syntax

```
change_cli_password parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| confirmpassword | String | Confirm the new password. |
| newpassword | String | The new password for this user. |
| username | String | The name of the user whose password you want to change. The name must be cli. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapic change_cli_password username=cli newpassword="Strong!Pass1234!" confirmpassword="Strong!Pass1234!"
```

Related reference

- [enable_strong_cli_password](#)

change_monitor_value

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/monitor_value
```

GuardAPI syntax

```
change_monitor_value parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|--|
| clusterName | String | Required. |
| parameter | String | Required. |
| value | Boolean | <p>Required. Valid values:</p> <ul style="list-style-type: none">• 0 (false)• 1 (true) <p>Default = 0 (false)</p> |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

change_rule_order

This command changes the order of a rule within a policy.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/change_rule_order
```

GuardAPI syntax

```
change_rule_order parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| fromPolicy | String | Required. The name of the policy. |
| order | Integer | Required. The new location for this rule within the policy. |
| ruleDesc | String | Required. The name of the rule to move. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapic change_rule_order ruleDesc="My policy exception1" fromPolicy="policy1" order=7
```

change_to_microsoft

This API is available in Guardium V12.0 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/changeToMicrosoft
```

GuardAPI syntax

```
change_to_microsoft parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| microsoftDriver | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

change_to_opensource

This API allows you to change the database driver ID from DataDirect to open source .

This API is available in Guardium v11.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/changeToOpensource
```

GuardAPI syntax

```
change_to_opensource parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|---|
| datasourceType | String | Required. For valid values, call <code>change_to_opensource</code> from the command line with <code>--help=true</code> . |
| opensourceDriver | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

change_tracker_get_events

Displays change tracker events. You can filter the request by hostname or task type.

For use by IBM Guardium support only.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/change_tracker_get_events
```

GuardAPI syntax

```
change_tracker_get_events parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| host | String | A hostname or IP address. |
| taskType | String | The type of task for which you want to display the events. For a list of available tasks, see change_tracker_get_tasks . |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Example

```
>grdapi change_tracker_get_events
ID=0
[
  {
    "unit": "my.company1.com",
    "events": [
      {
        "eventType": "IM_ALIVE_MSG",
        "eventDescription": "Unit not responding"
      }
    ],
    {
      "unit": "my.company2.com",
      "events": [
        {
          "eventType": "IM_ALIVE_MSG",
          "eventDescription": "Unit not responding"
        }
      ]
    }
]
```

Related reference

- [change_tracker_get_params](#)
- [change_tracker_get_tasks](#)
- [change_tracker_set_params](#)

change_tracker_get_params

Display the parameters for a specified change tracker task.

For use by IBM Guardium support only.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/change_tracker_get_params
```

GuardAPI syntax

```
change_tracker_get_params parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| paramName | String | The name of the parameter that you want to view. |
| task | String | A task for which you want to view the parameter names and values. For a list of available tasks, use the change_tracker_get_tasks API. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Example

```
grdapi change_tracker_get_params
ID=0
[
{
    "task": "CORE",
    "taskParams": [
        {"paramName": "CHANGE_TRACKER_ENABLED",
         "paramValues": [
             {"paramValue": "1"}
         ]},
        {"paramName": "CHANGE_TRACKER_MSG_QUEUE_SCAN_INTERVAL",
         "paramValues": [
             {"paramValue": "10"}
         ]},
        {"paramName": "CHANGE_TRACKER_MSG_QUEUE_CLEANSER_INTERVAL",
         "paramValues": [
             {"paramValue": "30"}
         ]},
        ...
    ],
    {
        "task": "UNIT_PROPERTIES",
        "taskParams": [
            {"paramName": "RUN_INTERVAL",
             "paramValues": [
                 {"paramValue": "300"}
             ]}
        ],
        {
            "task": "STAP_PROPERTIES",
            "taskParams": [
                {"paramName": "RUN_INTERVAL",
                 "paramValues": [
                     {"paramValue": "300"}
                 ]}
            ],
            {
                "task": "CUSTOM_EVENTS",
                "taskParams": [
                    {"paramName": "CERTIFICATE_EXPIRATION_ALERT_THRESHOLD",
                     "paramValues": [
                         {"paramValue": "365"}
                     ]}
                ],
                ...
            }
        }
    }
}
ok
```

Related reference

- [change_tracker_set_params](#)
- [change_tracker_reset](#)
- [change_tracker_get_tasks](#)

change_tracker_get_tasks

Display a list of the available change tracker tasks.

For use by IBM Guardium support only.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/change_tracker_get_tasks
```

GuardAPI syntax

```
change_tracker_get_tasks parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Example

Say something about the example

```
> grdapi change_tracker_get_tasks
ID=0
[
  {"task": "CORE"}, 
  {"task": "UNIT_PROPERTIES"}, 
  {"task": "STAP_PROPERTIES"}, 
  {"task": "UTILIZATION_THRESHOLD"}, 
  {"task": "REPORTING_TO_UNIT"}, 
  {"task": "UNIT_UTILIZATION"}, 
  {"task": "AWS_STREAM_STATUS"}, 
  {"task": "CUSTOM_EVENTS"}, 
  {"task": "MONITORED_STAPS"}, 
  {"task": "MSG_FORWARDING"}, 
  {"task": "STAP_VERIFICATION"}, 
  {"task": "MONITORED_TASK_EXECUTION"}, 
  {"task": "NANNY_HEALTH"}, 
  {"task": "IM_ALIVE"}, 
  {"task": "AGGREGATION"}, 
  {"task": "SCHEDULED_JOBS"}]
```

Related reference

- [change_tracker_get_params](#)
- [change_tracker_reset](#)
- [change_tracker_set_params](#)

change_tracker_reset

Reset the change tracker application to restart all of its internal tasks on the target host.

For use by IBM Guardium support only.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/change_tracker_reset
```

GuardAPI syntax

```
change_tracker_reset parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| host | String | Required. A host name or IP address. The host on which to restart the change tracker application. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

change_tracker_set_params

Set parameters for Guardium change tracker tasks.

For use by IBM Guardium support only.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/change_tracker_set_params
```

GuardAPI syntax

```
change_tracker_set_params parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| paramName | String | Required. The name of a parameter for the specified task. |
| paramValue | String | Required. The new value for the task parameter. |
| task | String | Required. The task for which you want to change a parameter value. For a list of available tasks, use the change_tracker_get_tasks API. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

The following command changes the RUN_INTERVAL parameter for the SCHEDULED_JOBS task to 62.

```
change_tracker_set_params task="SCHEDULED_JOBS"
paramName="RUN_INTERVAL"
paramValue="62"

curl -k --header "Authorization: Bearer bRVbgnfk0yfnJd1SVv6Mt532Zog" --include
--header "Content-Type: application/json" -X PUT --data
'{"task":"SCHEDULED_JOBS","paramName":"RUN_INTERVAL","paramValue":"62"}'
https://<appliance_hostname>:8443/restAPI/change_tracker_set_params
```

12.1 and later The following command sets the expiry threshold for certificates.

```
grdapic change_tracker_set_params
paramName=CERTIFICATE_EXPIRATION_ALERT_THRESHOLD
paramValue=365
task=CUSTOM_EVENTS
```

You need to update the CERTIFICATE_EXPIRATION_ALERT_THRESHOLD parameter across all managed units.

Related reference

- [change_tracker_get_events](#)
 - [change_tracker_get_params](#)
 - [change_tracker_get_tasks](#)
 - [change_tracker_reset](#)
-

clear_cas_template_set

Remove all templates from an existing Configuration Auditing System (CAS) template set.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/cas_template_set
```

GuardAPI syntax

```
clear_cas_template_set parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|---|
| templateSetLabel | String | Required. The name of the template set to clear. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

clevis_bind

Use this command to bind a managed unit to a tang server. Run this command on a central manager if you want to bind all managed units to the tang server.

This API is available in Guardium V11.3 and later.

GuardAPI syntax

```
clevis_bind parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| server | String | Required. The IP address of the tang server. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

clone_assessment

This command clones an existing assessment.

This API is available in Guardium v11.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/clone_assessment
```

GuardAPI syntax

```
clone_assessment parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------------------|------------|---|
| assessmentDescription | String | Required. The name of the existing assessment that is cloned. |
| newAssessmentDescription | String | The name of the cloned assessment. |

Examples

Example 1:

```
grdapiclone_assessment assessmentDescription=Assessment1 newAssessmentDescription=ClonedAssessment1
ID=20000
Created assessment ClonedAssessment1
ok
```

Example 2:

```
grdapiclone_assessment assessmentDescription=Assessment2
ID=20004
Created assessment COPY OF Assessment2
ok

grdapiclone_assessment assessmentDescription=Assessment2
ID=20005
Created assessment COPY 2 OF Assessment2
ok
```

Related reference

- [Assessment APIs](#)

clone_cas_template_set

This command creates a clone of an existing Configuration Auditing System (CAS) template set.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/clone_cas_template_set
```

GuardAPI syntax

```
clone_cas_template_set parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------------|------------|---|
| clonedTemplateSetLabel | String | Required. The name of the new template set. |
| templateSetLabel | String | Required. The name of the existing template set that you want to clone. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related concepts

- [Working with CAS Templates](#)

Related reference

- [Configuration Auditing System \(CAS\) APIs](#)

clone_extraction_profile

Clones a GBDI (Big Data) profile.

This API is available in Guardium V10.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/extractionProfile
```

GuardAPI syntax

```
clone_extraction_profile parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------------|------------|---|
| clone_profile_name | String | Required. The name of the new profile. |
| profile_name | String | Required. The profile you are cloning. For valid values run <code>grdapic get_extraction_profile_info</code> or call <code>clone_extraction_profile</code> from the command line with <code>--help=true</code> . |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To clone the profile Basic summary to a profile named Basics:

```
clone_extraction_profile profile_name=Basic summary clone_profile_name=Basics
```

Related concepts

- [Big Data Intelligence with data marts](#)

Related reference

- [Big Data Intelligence APIs](#)
-

clone_policy

This command clones an existing policy.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/clone_policy
```

GuardAPI syntax

```
clone_policy parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| clonedPolicyDes | String | Required. The name of the cloned policy. |
| policyDesc | String | Required. The name of the original policy. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi clone_policy policyDesc="Hadoop Policy" clonedPolicyDesc="My Hadoop Policy"
```

close_default_events

This command closes all of the events that are defined on a specific process, task, or execution for tasks of type *report*.

This command is useful if, for example, you have a task with a default event that returns numerous records, but the task cannot be signed unless all of the events are closed.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
close_default_events parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|--|
| eventStatus | String | Required. A final event status (such as Done). Must be a valid status for the default event that is defined for this audit task. |
| execDate | Date | Required. The execution date and time in the format <code>YYYY-MM-DD hh:mm:ss</code> . |
| processDesc | String | Required. The name of the audit process. |
| taskDesc | String | Required. The name of the audit task. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi close_default_events eventStatus=Done execDate="2020-03-01 08:00:00"
processDesc="Audit Process" taskDesc="Task Description"
```

configure_archive

Use this command to configure a data archive.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/configure_archive
```

GuardAPI syntax

```
configure_archive parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|--|
| accessKey | String | Required for Cleversafe; and for Amazon S3 when authType=Security-Credentials or authType=IAM-Role. Identifies user as the party responsible for service requests. It needs to be included in each request. It is not confidential and does not need to be encrypted. (20-character, alphanumeric sequence). |
| archiveOlderThan | Integer | Required. Specifies the number of days, older than which data is archived. For example, to archive data starting with yesterday's data, set this value to 1. |
| archiveValues | Integer | Required. Specify whether the archive data includes values from SQL strings. Valid values: <ul style="list-style-type: none"> • 0: no. Values are replaced with 'Value~Removed' in the archive, and are not available as part of a restore operation. • 1: yes. Values are maintained. |
| authType | String | Required for Amazon S3 only. Valid values: <ul style="list-style-type: none"> • Security-Credentials • IAM-Role • IAM-Instance-Profile |
| bucketName | String | Required for Amazon S3 and Cleversafe only. The unique bucket name. |
| destHost | String | Required for SCP, SFTP, Cleversafe only. Valid values: <ul style="list-style-type: none"> • SCP and SFTP: Host name of the target archive server. |
| ignoreOlderThan | Integer | Required. Together with archiveOlderThan, specifies the time interval of data to archive: data that is older than this value, in days, is not exported. |
| passwd | String | Required for SCP, SFTP. Valid values: Password for the target archive server. |
| passwdRetype | String | Required for SCP, SFTP. Password for the target archive server. |
| port | Integer | Required for SCP, SFTP only. Port on the target archive server. |
| protocol | String | Required. Protocol of the target destination.
For valid values, call configure_archive from the command line with <code>--help=true</code> . |

| Parameter | Value type | Description |
|-----------------|------------|---|
| region | String | Required for Amazon S3 only. Valid values: <ul style="list-style-type: none">• US_EAST_1• US_EAST_2• US_WEST_1• US_WEST_2• EU_CENTRAL_1• EU_WEST_1• EU_WEST_2• EU_WEST_3• EU_NORTH_1• CA_CENTRAL_1• AP_SOUTHEAST_1• AP_SOUTHEAST_2• AP_NORTHEAST_1• AP_NORTHEAST_2• SA_EAST_1• CN_NORTH_1• CN_NORTHWEST_1• AP_SOUTH_1• GovCloud• US_GOV_EAST_1 |
| retention | Integer | Required for Centera only. Number of days to retain the archive data on the target archive server. |
| roleARN | String | Required for Amazon S3 when authType=IAM-Role. The Amazon resource name (ARN) specifying this role. |
| secretKey | String | Required for Amazon S3 and Cleversafe only. The Secret Access Key is associated with the Access Key ID, used to calculate the digital signature that needs to be included in the request. (Only the user and AWS should have this 40-character sequence.) |
| ssh_key_active | Boolean | Enables data transfer using the SSH key. Enable the SSH key feature with the CLI command store system scp-ssh-key-mode on . Generate ssh-key pairs and copy the public part of the key, public-transfer-key , to the remote host. For more information, see Enabling ssh-key pairs for data archive, data export, data mart . Valid values: <ul style="list-style-type: none">• 0: Disable• 1: Enable Default = 0 |
| targetDir | String | Required for SCP, SFTP, Cleversafe only. Valid values: <ul style="list-style-type: none">• SCP, SFTP: The target directory on the target archive server.• Cleversafe: Authentication endpoint URL |
| userName | String | Required for SCP, SFTP only. User name for the target archive server. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To configure archive of data, with SQL strings, older than one day and younger than 2 days, on an SFTP server:

```
grdapi configure_archive archiveOlderThan=1 archiveValues=1 destHost=<full path to target archive host> ignoreOlderThan=2
passwd=pass1 passwdRetype=pass1 port=0 protocol=SFTP targetDir=/archive/dir

grdapi configure_archive archiveOlderThan=1 archiveValues=1 destHost="10.10.10.10" ignoreOlderThan=30 protocol="scp"
targetDir="/var/tmp" userName="root" ssh_keys_active=1
```

Related tasks

- [Managing stored data](#)

Related reference

- [Archive, export, import, purge, and restore APIs](#)

configure_data_streaming

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/dataStreaming
```

GuardAPI syntax

```
configure_data_streaming parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| dataToInclude | String | Valid values: <ul style="list-style-type: none">• <i>instance</i>• <i>exception</i>• <i>session</i>• <i>policy_violations</i>• <i>full_sql</i> |
| hostname | String | |
| PemKey | String | |
| port | Integer | |
| streamTo | String | Required. Valid values: <ul style="list-style-type: none">• <i>IBM_Security_Guardium</i>• <i>Guardium_Insights</i>• <i>Guardium_Big_Data_Intelligence</i>• <i>Datamart_For_Guardium_Insights</i> |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• <i>all_managed</i>: execute on all managed units but not the central manager• <i>all</i>: execute on all managed units and the central manager• <i>group:<group name></i>: execute on all managed units identified by <i><group name></i>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

configure_export

This command defines the data export to a Guardium® aggregator or central manager.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/configure_export
```

GuardAPI syntax

```
configure_export parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| aggHost | String | Required. The target aggregator hostname. |
| aggSecHost | String | The secondary target aggregator hostname. |
| exportOlderThan | Integer | Required. The export includes data older than this number of days. For example, to export yesterday's data and older data, set <code>exportOlderThan</code> to 1. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| exportValues | Integer | Required. Whether the export data includes values from SQL strings. Valid values: <ul style="list-style-type: none"> 0: no. Values are replaced with question mark characters in the export, and are not available as part of a restore operation. 1: yes |
| ignoreOlderThan | Integer | Required. Together with exportOlderThan, specifies the time interval of data to export: data that is older than this value, in days, is not exported. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> all_managed: execute on all managed units but not the central manager all: execute on all managed units and the central manager group:<group name>: execute on all managed units identified by <group name> host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To export data older than one day, but not older than 2 days, without the SQL strings, to the specified aggregator:

```
grdapic configure_export aggHost=<full path to target aggregator> exportOlderThan=1 exportValues=0 ignoreOlderThan=2
```

Related tasks

- [Exporting data](#)

Related reference

- [Archive, export, import, purge, and restore APIs](#)

configure_mfa

This command configures multi-factor authentication.

Before you run this command, make sure that your authentication application is configured. For DUO, define applications and users. For RSA SecurID, configure the RSA SecurID Authentication Manager.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/configure_mfa
```

GuardAPI syntax

```
configure_mfa parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|---|
| accessKey | String | RSA SecurID only.
From the RSA SecurID Console, generate the access key from the RSA SecurID Authentication API under Authentication Settings. |
| apiHost | String | The API host string. <ul style="list-style-type: none"> For DUO, the apiHost is from DUO. For RSA SecurID, the fully qualified domain name of the Authentication Manager. |
| clientId | String | RSA SecurID only.
The Hostname from the Add New Authentication Page of the RSA Security Console. |
| enable | Boolean | Required. Valid values: <ul style="list-style-type: none"> false: Disable multi-factor authentication. true: Enable multi-factor authentication. |
| exemptUsers | String | A comma-separated list of users to exempt from secondary authentication. You cannot exempt administrative OS (SSH) users. |
| iKey | String | DUO only. The integration key. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| loginPath | String | Required. Determines whether to provide multi-factor authentication to the Guardium GUI, CLI, or SSH. Valid values: <ul style="list-style-type: none"> • GUI: Guardium GUI • SET_GUIUSER: Guardium CLI • SSH: Guardium administrative OS users (cli and guardcli1 - guardcli9) who log in to the CLI via SSH. |
| mfaType | String | Required. The authentication type. . For valid values, call <code>configure_mfa</code> from the command line with <code>--help=true</code> . |
| port | Integer | RSA SecurID only. The communication port from the Add New Authentication Page of the RSA Security Console. The default is 5555. |
| sKey | String | DUO only. The secret key (from DUO). |
| verifySSL | Boolean | RSA SecurID only. Required for SSH users only. Determines whether to verify the server-side certificate for the RSA SecurID Authentication Manager. Before you run this command with <code>verifySSL='true'</code> , you need to upload the CA or self-signed certificate, which must be in PEM format. For more information, see either Configuring multi-factor authentication with RSA SecurID or store_certificate rsa_securid . Valid values: <ul style="list-style-type: none"> • <code>false</code>: Do not verify the SSL certificate. • <code>true</code>: Verify the SSL certificate. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> • <code>all_managed</code>: execute on all managed units but not the central manager • <code>all</code>: execute on all managed units and the central manager • <code>group:<group name></code>: execute on all managed units identified by <code><group name></code> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GuardAPI examples with DUO

This example configures multi-factor authentication for the Guardium GUI with DUO.

```
grdapi configure_mfa loginPath=GUI mfaType=DUO exemptUsers="admin, accessmgr" enable=true iKey=DIATOT8H1OXXXX
sKey=2gMRXVj2iQXXXX apiHost=api-ccccc.duosecurity.com
```

This example configures MFA with DUO for Guardium CLI users.

```
grdapi configure_mfa loginPath=SET_GUIUSER mfaType=DUO exemptUsers="admin, accessmgr" enable=true iKey=DINT141B9I2N91SXXXX
sKey=3gMRXVj2iQXXXX apiHost=api-ddddd.duosecurity.com
```

This example disables MFA with DUO for Guardium SSH users.

```
grdapi configure_mfa loginPath=SSH mfaType=DUO enable=false
```

GuardAPI examples with RSA SecurID

This example configures MFA for GUI users with RSA SecurID.

```
grdapi configure_mfa loginPath=GUI mfaType="RSA SecurID" exemptUsers="admin, accessmgr"
port=5555 verifySSL=false clientId=platform-vm10.mycompany.com
accessKey=t0qx4zg7agcd2gqtad414a353318i85808r428p5pbwgc33gn8381234567
apiHost=rsa88.mycompany.com enable=true
```

This example disables MFA for SSH users:

```
grdapi configure_mfa loginPath=SSH mfaType="RSA SecurID" enable=false
```

Related concepts

- [Configure multi-factor authentication](#).

configure_purge

Use this command to define a purge operation of data results on one or more Guardium® systems.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/configure_purge
```

GuardAPI syntax

```
configure_purge parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------------|------------|---|
| purgeAtAge | Integer | Required. Number of days after which results data is purged. |
| purgeWithoutArchive | Boolean | Required. Determines whether or not results data that has not been archived can be purged. For results data that are archived outside of your Guardium system, set to 1. Valid values: <ul style="list-style-type: none">• 0: no• 1: yes |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To purge results data after 2 days, but only if the results have been archived:

```
grdapi configure_purge purgeAtAge=2 purgeWithoutArchive=0
```

Related tasks

- [Managing stored data](#)

Related reference

- [Archive, export, import, purge, and restore APIs](#)

configure_results_archive

Use this API to configure the results archive on one or more Guardium® systems.

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/results_archive_comfiguration
```

GuardAPI syntax

```
configure_results_archive parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|---|
| accessKey | String | Required for Cleversafe; and for Amazon S3 when authType=Security-Credentials or authType=IAM-Role. Identifies user as the party responsible for service requests. It needs to be included it in each request. It is not confidential and does not need to be encrypted. (20-character, alphanumeric sequence). |
| archiveOlderThan | Integer | Required. The archive includes data older than this number of days. For example, to archive all data from yesterday and older than yesterday, set archiveOlderThan to 1. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| archiveValues | Integer | Required. Whether the archive data includes values from SQL strings. Valid values: <ul style="list-style-type: none"> 0: no. Values are replaced with question mark characters in the archive, and are not available as part of a restore operation. 1: yes |
| authType | String | Required for Amazon S3 only. Valid values: <ul style="list-style-type: none"> Security-Credentials IAM-Role IAM-Instance-Profile |
| bucketName | String | Required for Amazon S3 and Cleversafe only. The unique bucket name. |
| destHost | String | Host name of the target archive server. |
| ignoreOlderThan | Integer | Required. Together with archiveOlderThan, specifies the time interval of data to archive: data that is older than this value, in days, is not exported. |
| passwd | String | Required. Password for the target archive server. |
| passwdRetype | String | Required. Password for the target archive server. |
| port | Integer | Required. Port on the target archive server. |
| protocol | String | Required. For valid values, call configure_results_archive from the command line with --help=true. |
| region | String | Required for AmazonS3. Valid values: <ul style="list-style-type: none"> US_EAST_1 US_EAST_2 US_WEST_1 US_WEST_2 EU_CENTRAL_1 EU_WEST_1 EU_WEST_2 EU_WEST_3 EU_NORTH_1 CA_CENTRAL_1 AP_SOUTHEAST_1 AP_SOUTHEAST_2 AP_NORTHEAST_1 AP_NORTHEAST_2 SA_EAST_1 CN_NORTH_1 CN_NORTHWEST_1 AP_SOUTH_1 GovCloud US_GOV_EAST_1 |
| retention | Integer | Required for Centera only. Number of days to retain the archive data on the target archive server. |
| secretKey | String | Required for Amazon S3 and Cleversafe only. The Secret Access Key is associated with the Access Key ID, used to calculate the digital signature that needs to be included in the request. (Only the user and AWS should have this 40-character sequence.) |
| ssh_key_active | Boolean | Enables data transfer using the SSH key. Enable the SSH key feature with the CLI command store system scp-ssh-key-mode on . Generate ssh-key pairs and copy the public part of the key, public-transfer-key , to the remote host. For more information, see Enabling ssh-key pairs for data archive, data export, data mart . Valid values: <ul style="list-style-type: none"> 0: Disable 1: Enable Default = 0 |
| transferMethod | String | Required. Valid values: <ul style="list-style-type: none"> SCP FTP |
| targetDir | String | Required. The target directory on the target archive server. |
| userName | String | Required. User name for the target archive server. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> all_managed: execute on all managed units but not the central manager all: execute on all managed units and the central manager group:<group name>: execute on all managed units identified by <group name> host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123. host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To archive results older than 1 day but not older than 2 days, including the SQL strings, to an SCP server, with the username USER and password PASSW:

```
grdapi configure_results_archive archiveOlderThan=1 archiveValues=1 ignoreOlderThan=2 userName=USER passwd=PASSW  
passwdRetype=PASSW destHost=<full path to target archive host> port=<port> protocol=SCP targetDir=<directory on target archive  
server>
```

Related tasks

- [Managing stored data](#)

Related reference

- [Archive, export, import, purge, and restore APIs](#)

configure_results_export

This command defines the results export to Guardium® aggregators or central managers.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/configure_results_export
```

GuardAPI syntax

```
configure_results_export parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| destHost | String | Required. The target destination host name. |
| passwd | String | Required. Password for userName on the target destination host. |
| port | Integer | Required. Port on the target destination server. |
| protocol | String | Required. Valid values: <ul style="list-style-type: none">• SCP• FTP |
| ssh_key_active | Boolean | Enables data transfer using the SSH key. Enable the SSH key feature with the CLI command store system scp-ssh-key-mode on . Generate ssh-key pairs and copy the public part of the key, public-transfer-key , to the remote host. For more information, see Enabling ssh-key pairs for data archive, data export, data mart . Valid values: <ul style="list-style-type: none">• 0: Disable• 1: Enable Default = 0 |
| transferMethod | String | Required. Valid values: <ul style="list-style-type: none">• SCP• FTP |
| targetDir | String | Required. The target directory on the target destination server. |
| userName | String | Required. User name with write access for the target destination server. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To configure exporting of results older than one day, and not older than two days, using FTP, and where both username and password are admin:

```
grdapi configure_results_export destHost=<hostname of target> targetDir=<path to target directory> port=1111 userName=admin  
passwd=admin protocol=FTP
```

Related tasks

- [Exporting \(files\) results](#)

Related reference

- [Archive, export, import, purge, and restore APIs](#)

configure_system_backup

This API is available in Guardium v11.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/configure_system_backup
```

GuardAPI syntax

```
configure_system_backup parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| accessKey | String | |
| authType | String | |
| backupOptions | String | Required. Valid values: <ul style="list-style-type: none">• <code>cfg</code>• <code>data</code> |
| bucketName | String | |
| destHost | String | |
| passwd | String | |
| port | Integer | |
| protocol | String | Required. For valid values, call <code>configure_system_backup</code> from the command line with <code>--help=true</code> . |
| region | String | Valid values: <ul style="list-style-type: none">• <code>US_EAST_1</code>• <code>US_EAST_2</code>• <code>US_WEST_1</code>• <code>US_WEST_2</code>• <code>EU_CENTRAL_1</code>• <code>EU_WEST_1</code>• <code>EU_WEST_2</code>• <code>EU_WEST_3</code>• <code>EU_NORTH_1</code>• <code>CA_CENTRAL_1</code>• <code>AP_SOUTHEAST_1</code>• <code>AP_SOUTHEAST_2</code>• <code>AP_NORTHEAST_1</code>• <code>AP_NORTHEAST_2</code>• <code>SA_EAST_1</code>• <code>CN_NORTH_1</code>• <code>CN_NORTHWEST_1</code>• <code>AP_SOUTH_1</code>• <code>GovCloud</code>• <code>US_GOV_EAST_1</code> |
| retention | Integer | |
| roleARN | String | Valid values: <ul style="list-style-type: none">• <code>Security-Credentials</code>• <code>IAM-Role</code>• <code>IAM-Instance-Profile</code> |
| secretKey | String | |
| ssh_keys_active | Boolean | Valid values: <ul style="list-style-type: none">• <code>0</code> (false)• <code>1</code> (true) Default = 0 (false) |

| Parameter | Value type | Description |
|-----------------|------------|---|
| storageClass | String | Valid values: <ul style="list-style-type: none">• standard• glacier |
| targetDir | String | |
| userName | String | |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

copy_key_file

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/copy_key_file
```

GuardAPI syntax

```
copy_key_file parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| all | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true) <p>Default = 0 (false)</p> |
| fileName | String | Required. |
| targetUnit | String | |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

copy_rule

This command copies a specific rule from one policy to another policy.

Note: Both policies must exist.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/copy_rule
```

GuardAPI syntax

```
copy_rule parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| fromPolicy | String | Required. The name of the original policy. |
| ruleDesc | String | Required. The name of the rule to copy. |
| toPolicy | String | Required. The policy to which to copy the rule. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi copy_rule ruleDesc="My new rule" fromPolicy="policy1" toPolicy=" policy2 "
```

Related reference

- [copy_rules](#)

copy_rules

Copy all rules from one policy to another policy.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/copy_rules
```

GuardAPI syntax

```
copy_rules parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| fromPolicy | String | Required. The name of the original policy. |
| toPolicy | String | Required. The policy to which to copy the rule. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi copy_rules fromPolicy="policy1" toPolicy=" policy2 "
```

Related reference

- [copy_rule](#)

create_ad_hoc_audit_and_run_once

This command creates a new audit process report.

You can invoke this command automatically from any report.

When this command is invoked, it creates and runs a new audit process report. If such process for the user exists, then the parameters are updated and the same process is used. The behavior of this API is as follows:

- For a new process:
 1. The API creates one receiver per email in the sendToEmails list of the content type indicated in emailContentType.
 2. If includeUserReceiver parameter is set to true, the API also creates a user receiver for the user that is logged in
- For an existing process:
 1. All email receivers are removed and replaced with the emails from the new sendToEmails list (if any).
 2. If the list is empty, it removes all email receivers.
 3. If there is already a receiver for the user, it is not removed even if the includeUserreceiver is set to false. However if the parameter is true and there is no such receiver then it is added.

Once the audit process is generated, it is automatically executed (similar to a Run Once Now) and users should expect an item on their to-do list for that audit process.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/ad_hoc_audit_and_run_once
```

GuardAPI syntax

```
create_ad_hoc_audit_and_run_once parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------------|------------|---|
| changeParIfExist | Boolean | Required. Indicates whether to update the task parameters if the process exists. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| emailContentType | Integer | The type of content to send to users on the sendToEmails list. Valid values: <ul style="list-style-type: none">• 0: PDF• 1: CSV |
| includeUserReceiver | Boolean | Create a receiver for the logged-in user. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| isForReportRunOnce | Boolean | Required. Run the report once after it is created. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| processNameParam | String | If not blank, create a process with the specified name. |
| reportId | Integer | Required. The ID on the report to use for the only task in the Audit process. |
| sendToEmails | String | The email addresses of users to receive this report. A comma-separated list of email addresses. |
| taskParameter | String | All task parameters and their values concatenated with the characters ^^.
For example:

<code>PAR1=Val1^^PAR2=Val2^^</code>
You can leave a parameter empty. For example, to leave PAR2 empty: <code>PAR1=VAL1^^PAR2=^^PAR3=VAL3^^</code> |
| templateName | String | For valid values, call <code>create_ad_hoc_audit_and_run_once</code> from the command line with <code>--help=true</code> . |
| ticketAssignToGroup | String | If ticketReceiver is set to 1 (true), create an external ticket, assign the ticket to the specified group name or ID, and send the ticket to the external ticketing system (ServiceNow). |
| ticketAssignToMember | String | If ticketReceiver is set to 1 (true), create an external ticket, assign the ticket to the specified member name or ID, and send the ticket to the external ticketing system (IBM Resilient). |
| ticketAssignToUser | String | If ticketReceiver is set to 1 (true), create an external ticket, assign the ticket to the specified user name or ID, and send the ticket to the external ticketing system (ServiceNow). |

| Parameter | Value type | Description |
|----------------|------------|---|
| ticketReceiver | Boolean | If set to 1, add a receiver of type Ticket to the audit process result. When the audit process runs, Guardium creates a ticket and attaches the audit process result (as a PDF). Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| writeToSyslog | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |

Related tasks

- [Configuring an external ticketing system](#)

Related reference

- [Reports and report generation APIs](#)

create_ad_hoc_audit_and_run_with_name

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/ad_hoc_audit_and_run_once
```

GuardAPI syntax

```
create_ad_hoc_audit_and_run_with_name parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|---|
| changeParIfExist | Boolean | Required. Indicates whether to update the task parameters if the process exists. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| emailContentTy | Integer | The type of content to send to users on the sendToEmails list. Valid values: <ul style="list-style-type: none">• 0: PDF• 1: CSV |
| includeUserRec | Boolean | Create a receiver for the logged-in user. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| isForReportRun | Boolean | Required. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| processNamePa | String | If not blank, create a process with the specified name. |
| reportName | String | Required. For valid values, call <code>create_ad_hoc_audit_and_run_with_name</code> from the command line with <code>--help=true</code> . |
| sendToEmails | String | All task parameters and their values concatenated with the characters <code>^^</code> .
For example:

<code>PAR1=Val1^^PAR2=Val2^^</code>
You can leave a parameter empty. For example, to leave PAR2 empty: <code>PAR1=VAL1^^PAR2=^^PAR3=VAL3^^</code> |
| taskParameter | String | All task parameters and their values concatenated with the characters <code>^^</code> .
For example:

<code>PAR1=Val1^^PAR2=Val2^^</code>
You can leave a parameter empty. For example, to leave PAR2 empty: <code>PAR1=VAL1^^PAR2=^^PAR3=VAL3^^</code> |
| templateName | String | For valid values, call <code>create_ad_hoc_audit_and_run_with_name</code> from the command line with <code>--help=true</code> . |
| ticketAssignToG | String | If ticketReceiver is set to 1 (true), create an external ticket, assign the ticket to the specified group name or ID, and send the ticket to the external ticketing system (ServiceNow). |

| Parameter | Value type | Description |
|----------------------|------------|--|
| ticketAssignToMember | String | If ticketReceiver is set to 1 (true), create an external ticket, assign the ticket to the specified member name or ID, and send the ticket to the external ticketing system (IBM Resilient). |
| ticketAssignToUser | String | If ticketReceiver is set to 1 (true), create an external ticket, assign the ticket to the specified user name or ID, and send the ticket to the external ticketing system (ServiceNow). |
| ticketReceiver | Boolean | If set to 1, add a receiver of type Ticket to the audit process result. When the audit process runs, Guardium creates a ticket and attaches the audit process result (as a PDF). Valid values: <ul style="list-style-type: none"> • 0 (false) • 1 (true) Default = 0 (false) |
| writeToSyslog | Boolean | Valid values: <ul style="list-style-type: none"> • 0 (false) • 1 (true) Default = 0 (false) |

Related tasks

- [Configuring an external ticketing system](#)

Related reference

- [Reports and report generation APIs](#)

create_ad_hoc_audit_for_security_assessment

This API creates a security assessment (and if needed, an audit process) for one or more specified datasources.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/ad_hoc_audit_for_security_assessment
```

GuardAPI syntax

```
create_ad_hoc_audit_for_security_assessment parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------------|------------|--|
| datasourcesParam | String | A list of comma-separated datasource IDs. The security assessment runs all available tests of each datasource based on the datasource type. |
| includeUserReceiver | Boolean | Create a receiver for the logged-in user. Valid values: <ul style="list-style-type: none"> • 0 (false) • 1 (true) |
| processNameParam | String | The name of the audit process. If you do not specify an audit process name, Guardium creates the audit process and security assessment with the following names: <ul style="list-style-type: none"> • Audit process - Audit_SA_U_userId. • Security assessment - SA_U_userId. If you specify an audit process name, Guardium checks to see whether a security assessment with the same name as the audit process exists. If an audit process exists, but a security assessment does not, Guardium creates the security assessment. |
| sendToEmails | String | The type of content to send to users on the sendToEmails list. Valid values: <ul style="list-style-type: none"> • 0: PDF • 1: CSV |
| ticketAssignToGroup | String | If ticketReceiver is set to 1 (true), create an external ticket, assign the ticket to the specified group name or ID, and send the ticket to the external ticketing system (ServiceNow). |
| ticketAssignToMember | String | If ticketReceiver is set to 1 (true), create an external ticket, assign the ticket to the specified member name or ID, and send the ticket to the IBM Resilient external ticketing system. |
| ticketAssignToUser | String | If ticketReceiver is set to 1 (true), create an external ticket, assign the ticket to the specified username or ID, and send the ticket to the ServiceNow external ticketing system. |

| Parameter | Value type | Description |
|----------------|------------|---|
| ticketReceiver | Boolean | If set to 1, add a receiver of type Ticket to the audit process result. When the audit process runs, Guardium creates a ticket and attaches the audit process result (as a PDF). Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |

Example

For this example, `datasourcesPar=20000` represents the DATASOURCE_ID of an existing Guardium security assessment datasource.

```
grdapi create_ad_hoc_audit_for_security_assessment processNamePar=psa datasourcesPar=20000
sendToEmails="joan.darcy@mycompany.com" ticketReceiver=1 ticketAssignToGroup="database"
```

Related tasks

- [Configuring an external ticketing system](#)

Related reference

- [Reports and report generation APIs](#)

create_adhoc_policy_analyzer

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/create_adhoc_policy_analyzer
```

GuardAPI syntax

```
create_adhoc_policy_analyzer parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| date | String | Required. |
| duration | String | Required. |
| unit | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

create_alias

Use this command to create or update a meaningful name for a data value or object in reports or queries.

Use `create_alias` to add a meaningful (or user-friendly) synonym to any of the objects listed in the `groupTypeDesc` parameter field.

For more information about using aliases, see [Aliases](#).

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/alias
```

GuardAPI syntax

```
create_alias parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| aliasValue | String | Required. The alias for the object or data value. |
| dbValue | String | Required. The name of the database or other value for which you are creating an alias. |
| groupTypeDesc | String | Required. The type of object for which you are creating the alias. For valid values, call <code>create_alias</code> from the command line with <code>--help=true</code> . |
| overrideIfExist | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false) Default.• 1 (true)• If set to 1:<ul style="list-style-type: none">◦ If an alias does not exist for the specified object, the alias is created.◦ If the specified object already has an alias, the alias for that object is updated to the new alias name.• If set to 0, Guardium returns an error message if an alias exists for the object. |

GuardAPI example

```
grdapi create_alias aliasValue="New Central Manager" dbValue=1 groupTypeDesc="Server Hostname"
```

Related concepts

- [Aliases](#)

Related reference

- [delete_alias](#)
- [list_aliases](#)
- [update_alias](#)

create_allowed_db

This command creates a User-DB association.

Note: To apply the changes to the active User-DB association map, run [update_user_db](#) after you run this command.
This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/allowed_db
```

GuardAPI syntax

```
create_allowed_db parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------|------------|---|
| instanceName | String | A specific instance name within the server. |
| serverIp | String | Required. The server IP. |
| userName | String | Required. The name of the user. |

Examples

```
grdapi create_allowed_db userName=Fred serverIp=192.168.1.1 instanceName=test
```

Related concepts

- [Data Security - User Hierarchy and Database Associations](#)

Related reference

- [update_user_db](#)

create_api_key

12.1 and later This command creates an API key for a Guardium user.

GuardAPI syntax

```
create_api_key parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| name | String | Required. The name of the API key must not contain the "-" character. |
| username | String | If not specified, the username is set to the logged-in user. If specified, the logged-in user must have the accessmgr role to associate the API key to the username. |

GuardAPI example

The following example shows the command to create an API key VAScanner_IT for the *admin* user.

```
grdapi create_api_key name=VAScanner_IT username=admin
```

create_api_parameter_mapping

Guardium® includes a battery of predefined reports. Many reports are mapped to GuardAPI functions to ease configuration. Use this command to define additional reports, including custom reports, and map them to GuardAPI functions for each report.

For more information about mapping GuardAPIs to domains, entities, and attributes, see [Mapping APIs to report results](#).

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/param_mapping_for_function
```

GuardAPI syntax

```
create_api_parameter_mapping parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| attributeLabel | String | Required. An attribute within an entity. |
| domain | String | Required. One of the Guardium reporting domains such as Access, Alert, Discovered Instances, Exceptions, or Group Tracking. |
| entityLabel | String | Required. The name of the entity within the reporting domain. |
| functionName | String | Required. The API function to map. |
| parameterName | String | Required. The parameter within the API. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GuardAPI example

```
grdapi create_api_parameter_mapping functionName="create_group" parameterName="desc" domain="Group Tracking"
entityLabel="Group" attributeLabel="Group Description"
```

Related concepts

- [Mapping APIs to report results](#)

create_assessment

This command adds a security assessment.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/assessment
```

GuardAPI syntax

```
create_assessment parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|---|
| assessmentDescription | String | Required. A unique variable to describe the assessment. |
| processName | String | |

Example

```
grdapi create_assessment assessmentDescription=Assess1
```

create_autodetect_process

Use this command to create an auto-discovery process.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/autodetect_processes
```

GuardAPI syntax

```
create_autodetect_process parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------------|------------|--|
| check_ICMP_echo | Boolean | Required. Whether or not Nmap sends an ICMP echo request. PE parameter to nmap. This is an nmap parameter. nmap options are configurable only by API (not by GUI). For details of nmap parameters and their impact on scan performance, see man nmap. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| host_timeout | Integer | Required. Timeout value, in seconds, for determining how long Guardium waits for a probe response before giving up or retransmitting the probe. This is an nmap parameter. nmap options are configurable only by API (not by GUI). For details of nmap parameters and their impact on scan performance, see man nmap. |
| process_name | String | Required. Name of the auto-discovery process |
| run_probe_after_scan | Boolean | Required. Determines whether or not to run a probe job immediately after the scan job completes. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |

| Parameter | Value type | Description |
|-----------------|------------|---|
| use_dns | String | Required. This is an nmap parameter. nmap options are configurable only by API (not by GUI). For details of nmap parameters and their impact on scan performance, see man nmap. Valid values: <ul style="list-style-type: none"> <i>true</i>: always <i>false</i>: never <i>n</i>: never <i>R</i>: always |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> <i>all_managed</i>: execute on all managed units but not the central manager <i>all</i>: execute on all managed units and the central manager <i>group:<group name></i>: execute on all managed units identified by <i><group name></i> host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To create a process named myProcess in the Guardium system on which you enter the command:

```
grdapi create_autodetect_process process_name=myProcess check_ICMP_echo=false host_timeout=3 run_probe_after_scan=false
use_dns=n
```

Related concepts

- [Database auto-discovery](#)

Related reference

- [Auto-discovery APIs](#)

create_aws_secrets_manager_config

Use this command to create an AWS secrets configuration for your authentication scenario. You can create a configuration using security credentials, IAM role, or IAM instance profile.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/aws_secrets_manager
```

GuardAPI syntax

```
create_aws_secrets_manager_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------------|------------|---|
| access_key_id | String | |
| auth_type | String | Required. Valid values: <ul style="list-style-type: none"> <i>Security-Credentials</i> <i>IAM-Role</i> <i>IAM-Instance-Profile</i> |
| name | String | Required. |
| role_arn | String | The Role Amazon Resource Name (ARN) |
| secret_access_key | String | |
| secret_key_password | String | The Secret key label for the password |
| secret_key_username | String | The Secret key label for the username |

Examples

Create an AWS secrets configuration using security credentials

```
grdapi create_aws_secrets_manager_config name="GRDAPI Security-Credentials" auth_type="Security-Credentials"  
access_key_id="home_markdown_jenkins_workspace_Transform_in_SSMPHH_12.x_com.ibm.guardium.doc.reference_grdapi_create_aws_secre  
ts_manager_config_ABCD123" secret_access_key="XYZ321" secret_key_password="password" secret_key_username="username"
```

Create an AWS secrets configuration using IAM role

```
grdapi create_aws_secrets_manager_config name="GRDAPI IAM-Role" auth_type="IAM-Role"  
access_key_id="home_markdown_jenkins_workspace_Transform_in_SSMPHH_12.x_com.ibm.guardium.doc.reference_grdapi_create_aws_secre  
ts_manager_config_ABCD123" secret_access_key="XYZ321"  
role_arn="arn:aws:iam::123456789:role/AWS_Secret_ManagerReadWrite_role" secret_key_password="password"  
secret_key_username="username"
```

Create an AWS secrets configuration using IAM instance profile

```
grdapi create_aws_secrets_manager_config name="GRDAPI IAM-Instance-Profile1" auth_type="IAM-Instance-Profile1"  
secret_key_password="password" secret_key_username="username"
```

create_cas_host_instance

Creates a Configuration Auditing System (CAS) host instance. Each host instance can define one or more CAS instances, which specify a CAS template set, and defines the parameters that are needed to connect to the database.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/cas_host_instance
```

GuardAPI syntax

```
create_cas_host_instance parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|---|
| datasourceName | String | Required. The data source to use for this host instance. |
| templateSetLabel | String | Required. The name of the template set to associate with the host. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

REST API example

To create a CAS host instance associated with the `cas_temp_set_001` template set:

```
curl -k --header "Authorization:Bearer 8ad14246-8815-4043-ab19-074d6bfcaad3" -i -X  
POST -d '{"datasourceName":"DB_for_CAS","templateSetLabel":"cas_temp_set_001"}'  
https://localhost:8443/restAPI/cas_host_instance
```

Related concepts

- [CAS Hosts](#)

Related reference

- [Configuration Auditing System \(CAS\) APIs](#)

create_cas_template

This command creates a Configuration Auditing System (CAS) template item. A template, or template item is a specific file or file pattern, environment or registry variable, the output of an OS or SQL script, or a list of logged-in users.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/cas_template
```

GuardAPI syntax

```
create_cas_template parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|---|
| auditType | String | Required. The type of item to monitor. Valid values: <ul style="list-style-type: none">• ENV_VAR: Environment variable• FILE• FILE_PAT: File pattern• OS_SCRIPT: OS script• REG_VAR: Registry variable• REG_PAT: Registry variable pattern• SQL query |
| enabled | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true): The template is enabled after you create it. |
| isEditable | Boolean | This template can be modified. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true): This template can be modified. |
| period | Integer | The number of minutes between tests. |
| saveData | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true): Previous versions of the item can be compared with the current version. |
| template | String | Required. The name of this template. |
| templateSetLabel | String | Required. The name of the template set to associate with this template. |
| useMD5 | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true): Guardium uses the MD5 algorithm to calculate a checksum and compare the latest value with the value calculated the last time that the item was checked. Default = 0 |

REST API example

To add a CAS template to a CAS template set:

```
curl -k --header "Authorization: Bearer 8ad14246-8815-4043-ab19-074d6bfcaad3" -i -X  
POST -d  
'{"auditType":"File","template":"$DB2_HOME/sqlLIB/db2nodes.cfg","templateSetLabel":"cas_temp_set_001","saveData":true}'  
https://localhost:8443/restAPI/cas_template
```

Related concepts

- [CAS Templates domain](#)
- [Configuration Auditing System \(CAS\)](#)

Related reference

- [Configuration Auditing System \(CAS\) APIs](#)

create_cas_template_set

This command creates a template set for the Configuration Auditing System (CAS).

A CAS template set contains a list of item templates that are bundled together. Each CAS template set shares a common purpose such as monitoring a particular type of database (such as Oracle on UNIX). A database template set is always specific to both the database type and the operating system type.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/cas_template_set
```

GuardAPI syntax

```
create_cas_template_set parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|---|
| dbType | String | Required. The database type.
If you enter a database type that is not supported (or you misspell it), Guardium displays a list of supported DBs. If the template set does not require a specific DB type, specify N_A. |
| isDefault | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true): This template set is the default. |
| isEditable | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true): This template set can be modified. |
| osType | String | Required. The operating system type can be either: <ul style="list-style-type: none">• UNIX: UNIX• WIN: Windows |
| templateSetLabel | String | Required. The name of this template set. |

REST API Example

To create a CAS template set for Db2 on UNIX:

```
curl -k --header "Authorization:Bearer 8ad14246-8815-4043-ab19-074d6bfcaad3" -i -X POST -d '{"dbType":"DB2","osType":"UNIX","templateSetLabel":"cas_temp_set_001"}' https://localhost:8443/restAPI/cas_template_set
```

Related concepts

- [Working with CAS templates](#)

Related reference

- [Configuration Auditing System \(CAS\) APIs](#)

create_classifier_action

This command creates classification actions.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/classifier_action
```

GuardAPI syntax

```
create_classifier_action parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| | | |

| Parameter | Value type | Description |
|---------------------|------------|---|
| accessPolicy | String | |
| accessRuleAction | String | |
| actionName | String | Required. |
| actionType | String | Required. For valid values, call <code>create_classifier_action</code> from the command line with <code>--help=true</code> . |
| actualMemberContent | String | |
| commandsGroup | String | |
| description | String | |
| excludeObjectGroup | String | |
| includeField | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true) <p>Default = 0 (false)</p> |
| includeServerIP | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true) <p>Default = 0 (false)</p> |
| notificationType | String | |
| objectFieldGroup | String | |
| objectGroup | String | |
| policyName | String | Required. |
| privacySet | String | |
| receiver | String | |
| replaceGroupContent | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true) <p>Default = 0 (false)</p> |
| ruleDescription | String | |
| ruleName | String | Required. |
| SchemaGroup | String | |
| severity | String | |

create_classifier_document_rule

This API is available in Guardium v11.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/classifier_document_rule
```

GuardAPI syntax

```
create_classifier_document_rule parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------------------|------------|---|
| calculateConfidenceScore | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true) <p>Default = 0 (false)</p> |
| category | String | Required. For valid values, call <code>create_classifier_document_rule</code> from the command line with <code>--help=true</code> . |
| classification | String | Required. |
| collectionNameLike | String | |
| collectionTypeCollection | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true) <p>Default = 1 (true)</p> |

| Parameter | Value type | Description |
|--------------------------------|------------|---|
| collectionTypeView | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| compareToValuesInGroup | String | |
| compareToValuesInSQL | String | |
| continueOnMatch | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| continueWithUnmatchedFieldOnly | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| dataTypes | String | |
| description | String | |
| evaluationName | String | |
| excludeCollection | String | |
| excludeCollectionField | String | |
| excludeDatabaseName | String | |
| fieldNameLike | String | |
| fireOnlyWithMarker | String | |
| hitPercentage | Integer | |
| policyName | String | Required. |
| ruleName | String | Required. |
| ruleType | String | Required. For valid values, call <code>create_classifier_document_rule</code> from the command line with <code>--help=true</code> . |
| searchExpression | String | |
| searchLike | String | |
| showUniqueValues | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| skipEmptyNull | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| uniqueValueMask | String | |

create_classifier_policy

This command creates classification policies.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/classifier_policy
```

GuardAPI syntax

```
create_classifier_policy parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|--|
| category | String | Required. For valid values, call <code>create_classifier_policy</code> from the command line with <code>--help=true</code> . |
| classification | String | Required. |
| description | String | |
| policyName | String | Required. |

Examples

```
grdapi create_classifier_policy policyName=access_policy classification=class1 description="Access policy" category=Access
```

create_classifier_process

This command creates classification processes.

Use **create_classifier_process** after creating a classification policy and datasource.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/classifier_process
```

GuardAPI syntax

```
create_classifier_process parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|--|
| comprehensive | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| datasourceGroups | String | |
| datasourceNames | String | |
| datasourceType | String | Valid values: <ul style="list-style-type: none">• DOCUMENT• RELATIONAL Default = RELATIONAL |
| includeInternalTables | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false)

Enabling includeInternalTables indicates that you want to scan internal system databases and schema used by the database software provider. Internal system databases and schema are unlikely to contain sensitive data and are not scanned by default. When including internal tables, verify that the classifier datasource user has sufficient privileges to scan the internal databases and schema. Insufficient privileges may result in unexpected classification policy errors.

To view and edit the databases and schema impacted by the includeInternalTables parameter, use the Group Builder to edit one of the predefined Excluded Classification groups. |
| policyName | String | Required. |
| processName | String | Required. |
| sampleSize | Integer | |

Examples

```
grdapi create_classifier_process datasourceNames=sample_cls_0001 policyName=APITEST_Cls_Ply_10001_1  
processName=APITEST_Clps_10001_1
```

create_classifier_rule

This command creates classification rules.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

POST https://[Guardium hostname or IP address]:8443/restAPI/classifier_rule

GuardAPI syntax

```
create_classifier_rule parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------------------------|------------|--|
| calculateConfidenceScore | Boolean | Calculate a confidence score. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| category | String | Required. For valid values, call create_classifier_rule from the command line with --help=true. |
| classification | String | Required. |
| columnNameLike | String | |
| compareToValuesInGroup | String | |
| compareToValuesInSQL | String | |
| continueOnMatch | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| continueWithUnmatchedColumnsOnly | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| dataTypes | String | |
| description | String | |
| evaluationName | String | |
| excludeSchemaName | String | |
| excludeTable | String | |
| exclude TableColumn | String | |
| fireOnlyWithMarker | String | |
| hitPercentage | Integer | |
| maxLength | Integer | |
| minLength | Integer | |
| policyName | String | Required. |
| ruleName | String | Required. |
| ruleType | String | Required. For valid values, call create_classifier_rule from the command line with --help=true. |
| searchExpression | String | |
| searchLike | String | |
| showUniqueValues | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| skipEmptyNull | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| tableNameLike | String | |
| tableTypeSynonym | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| tableTypeSystemTable | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| tableTypeTable | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |

| Parameter | Value type | Description |
|-----------------|------------|--|
| tableTypeView | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| uniqueValueMask | String | |

create_cloudTitle

This API creates or defines a cloud service account.

Use `create_cloudTitle` to create or define a cloud database service account from the command line or by using a REST API. For more information, see [Cloud database service protection](#).

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/create_cloud_datasource
```

GuardAPI syntax

```
create_cloudTitle parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------------|------------|---|
| access_key_id | String | The access key ID supplied by your cloud service provider. |
| audit_type | String | Valid values: <ul style="list-style-type: none">• <i>dataStream</i>• <i>native</i> Defines the audit type: <ul style="list-style-type: none">• To use data streams, specify <i>dataStream</i>.• To use native audit, specify <i>native</i>. |
| auth_type | String | Required for Amazon only. Valid values: <ul style="list-style-type: none">• <i>Security-Credentials</i>• <i>IAM-Role</i>• <i>IAM-Instance-Profile</i> |
| classification_process | String | For native audit only, optionally specify a classification process. |
| name | String | Required. An account name that is unique to your site. |
| object_limit | Integer | For native audit only, specify the maximum number of objects that are found in the classification process that are added automatically to the list of audited objects. |
| provider | String | Valid values: <ul style="list-style-type: none">• <i>Amazon</i>• <i>Azure</i> |
| role_arn | String | For Amazon only, the Amazon resource name (ARN) for this role. |
| secret_access_key | String | The secret access key ID supplied by your cloud service provider. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• <i>all_managed</i>: execute on all managed units but not the central manager• <i>all</i>: execute on all managed units and the central manager• <i>group:<group name></i>: execute on all managed units identified by <i><group name></i>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Related concepts

- [Cloud database service protection](#)

create_cloud_datasource

This command creates a cloud datasource, for classification, vulnerability assessment, and object auditing on cloud databases (cloud database service protection).

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/cloud_datasource
```

GuardAPI syntax

```
create_cloud_datasource parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------------|------------|--|
| application | String | Required. The application type to be used with this data source. For valid values, call <code>create_cloud_datasource</code> from the command line with <code>--help=true</code> . |
| cloudTitle | String | Required. Name of a cloud account already defined in Guardium. For valid values, call <code>create_cloud_datasource</code> from the command line with <code>--help=true</code> .
For more information, see create_cloudTitle . |
| compatibilityMode | String | The mode used when monitoring a table. |
| conProperty | String | Use only if additional connection properties must be included on the JDBC URL to establish a JDBC connection with this data source. The required format is <code>property=value</code> , where each property and value pair is separated by a comma. |
| customURL | String | Connection string to the data source. If not provided the connection is made by using the host, port, instance, and other properties of the previously entered fields. You can, for example, use this method to create Oracle Internet Directory (OID) connections. |
| cyberarkConfigName | String | The name of the CyberArk configuration on your Guardium system. For valid values, call <code>create_cloud_datasource</code> from the command line with <code>--help=true</code> . |
| cyberarkObjectName | String | The CyberArk object name for the Guardium datasource. |
| dbInstanceAccount | String | Database Account Login Name that is used by the Configuration Auditing System (CAS). |
| dbInstanceDirectory | String | Directory where database software is installed that is used by CAS. |
| dbName | String | For a Db2® or Oracle data source, enter the schema name. For others, enter the database name. |
| description | String | Longer description of the data source. |
| externalPasswordType | String | For valid values, call <code>create_cloud_datasource</code> from the command line with <code>--help=true</code> . |
| host | String | Required. The hostname or the IP address of the server that is hosting the DB you are monitoring. |
| importServerSSLcert | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| KerberosConfigName | String | Name of Kerberos configuration already defined in Guardium system. |
| name | String | Required. A unique name for the data source in the Guardium system. |
| objectLimit | Integer | Required. The maximum number of sensitive objects found in the classification process that are added automatically to the list of audited objects. Default = 20. |
| password | String | Password for user. |
| port | Integer | Port number. |
| primaryCollector | Integer | The collector that extracts the audit data from the cloud database. |
| region | String | Required for AWS only. For valid values, call <code>create_cloud_datasource</code> from the command line with <code>--help=true</code> . |
| savePassword | Boolean | Saves and encrypts your authentication credentials on the Guardium appliance. Required if you are defining a data source with an application that runs as a scheduled task (as opposed to on demand). When set to yes, login name and password are required. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| serviceName | String | Required for Oracle, Informix®, Db2, and IBM® i. For a Db2 data source, enter the database name; for others, enter the service name. |

| Parameter | Value type | Description |
|---------------------|------------|---|
| severity | String | Severity Classification (or impact level) for the data source. For valid values, call create_cloud_datasource from the command line with <code>--help=true</code> . |
| shared | String | Set to <code>true</code> or <code>Shared</code> to share with other applications. To share the data source with other users, you need to assign roles from the GUI. Valid values: <ul style="list-style-type: none"> <code>Shared</code> <code>Not Shared</code> <code>true</code> <code>false</code> |
| type | String | Required. Identifies the data source type. For valid values, call create_cloud_datasource from the command line with <code>--help=true</code> . |
| useExternalPassword | Boolean | Valid values: <ul style="list-style-type: none"> <code>0</code> (false) <code>1</code> (true) |
| useKerberos | Boolean | Set to yes to use Kerberos authentication. If yes, KerberosConfigName must be supplied. Valid values: <ul style="list-style-type: none"> <code>0</code> (false) <code>1</code> (true) |
| useLDAP | Boolean | Set to yes to use LDAP. Valid values: <ul style="list-style-type: none"> <code>0</code> (false) <code>1</code> (true) |
| user | String | User for the data source. If used, password must also be used. |
| useSSL | Boolean | Set to yes to use SSL authentication. Valid values: <ul style="list-style-type: none"> <code>0</code> (false) <code>1</code> (true) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> <code>all_managed</code>: execute on all managed units but not the central manager <code>all</code>: execute on all managed units and the central manager <code>group:<group name></code>: execute on all managed units identified by <code><group name></code> host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

This example defines a cloud data source that is named cloud9, associated with cloud account NYSW, by using the access policy application.

```
grdapicreate_cloud_datasource cloudTitle=nysw application="Access Policy" host=11.11.11.11 name=cloud9 primaryCollector=coll56
region=ca-central-1 type="Oracle (DataDirect - SID)"
```

Related concepts

- [Cloud database service protection](#)

create_computed_attribute

This API creates a custom attribute that is calculated based on a specified expression. The computed attribute is then available for reporting.

To help prevent an SQL injection attack, the following words and characters are not allowed in computed attributes:

ALTER, CREATE, DELETE, DROP, INSERT, TRUNCATE, UPDATE, semicolon (;), double-dash (--), or slash-asterisk /*)

To replace the disallowed characters, you can use the MySQL char function. For example, say that you want to create a computed attribute that includes a semicolon. The API call that includes a semicolon:

```
grdapicreate_computed_attribute
attributeLabel="app_user" entityLabel="Access Period"
expression="SUBSTRING_INDEX(APP_USER_NAME,';',1)"
```

Returns the following error:

```
create_computed_attribute:
ERR=2410
```

Error Creating New Computed Attribute - Invalid Expression Or expression includes not allowed characters

To correct the example, use the MySQL char function (where 59 is the code for a semicolon):

```
grdapi create_computed_attribute  
attributeLabel="app_user" entityLabel="Access Period"  
expression="SUBSTRING_INDEX(APP_USER_NAME,char(59),1)"
```

Which returns the following information:

```
ID=20000  
Attribute for Expression SUBSTRING_INDEX(APP_USER_NAME,char(59),1) Created
```

The char() equivalents are shown in [Table 1](#).

Table 1. MySQL character equivalents

| Character | MySQL char() |
|---------------------|---------------|
| ; (semicolon) | char (59) |
| -- (double dash) | char (45, 45) |
| /* (slash asterisk) | char (47, 42) |

This API is available in Guardium V9.5 and later.

The REST API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/computed_attribute
```

GuardAPI syntax

```
create_computed_attribute parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|---|
| attributeLabel | String | Required. The name of the computed attribute, which appears in reports. |
| entityLabel | String | Required. The name of the main entity with which the attribute is associated, for example Session, Object, or FULL_SQL. |
| expression | String | Required. An SQL expression to generate the computed value for the new attribute. |

Examples

To create a computed attribute called app_user associated with the Access Period entity:

```
grdapi create_computed_attribute  
attributeLabel="app_user" entityLabel="Access Period"  
expression="SUBSTRING_INDEX(APP_USER_NAME,char(59),1)"
```

To create an Oracle_OS_user attribute associated with the Session entity:

```
grdapi create_computed_attribute  
attributeLabel="Oracle_OS_User" entityLabel="Session"  
expression="SUBSTRING_INDEX( SUBSTRING(REPLACE(UID_CHAIN,' ',''),1,LENGTH(REPLACE(UID_CHAIN,' ','')) - LOCATE('lqsi',REVERSE(REPLACE(UID_CHAIN,' ','')))-4),' ',1)"
```

Related reference

- [list_computed_attribute](#)

create_constant_attribute

Defines a custom attribute that has a constant value.

This API is available in Guardium V9.5 and later.

The REST API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/constant_attribute
```

GuardAPI syntax

```
create_constant_attribute parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|---|
| attributeLabel | String | Required. The name of the attribute, which appears in reports. |
| constant | String | Required. The value of this attribute, which can be any constant value. |
| entityLabel | String | Required. The name of the main entity with which the attribute is associated, for example Session, Object, or FULL_SQL. |

create_custom_table_ldap_import

This command configures a custom table to import data from LDAP.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/custom_data_ldap
```

GuardAPI syntax

```
create_custom_table_ldap_import parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------------------------|--|
| activateSchedule | Boolean-Constant values list | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| attributeMapping | String | Required. |
| baseDN | String | Required. |
| clearTable | Boolean-Constant values list | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| cronString | String | |
| filter | String | |
| filterScope | String | Valid values: <ul style="list-style-type: none">• one-level• sub-tree |
| hostName | String | Required. |
| importLimit | Integer | |
| password | String | |
| port | Integer | Required. |

| Parameter | Value type | Description |
|-----------------|-------------------------------------|---|
| serverType | String | Required. Valid values: <ul style="list-style-type: none"> • Active Directory • Novell Directory • Open LDAP • Sun ONE Directory • z/OS Security Server • Tivoli Directory |
| startDate | Date | |
| tableName | String | Required. |
| userName | String | |
| useSSL | Boolean-
Constant values
list | Valid values: <ul style="list-style-type: none"> • 0 (false) • 1 (true) Default = 0 (false) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

create_cyberark_config

This command configures the CyberArk application IDs on your Guardium system. Obtain the application IDs, corresponding safe names, and folder names from your CyberArk administrator.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/cyberark
```

GuardAPI syntax

```
create_cyberark_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------|------------|--|
| applicationId | String | Required. This is a unique variable that is created on CyberArk. |
| folderName | String | Required. The name of the folder where the CyberArk safe is located. |
| name | String | Required. The name that is used to configure the Guardium datasource to access the CyberArk vault. |
| safeName | String | Required. The name of the CyberArk safe that is assigned to the <code>applicationId</code> . |

create_datasource

Use this command to define new on-premises datasources.

Important: In a centrally-managed environment, datasources must be defined on the central manager. Datasources that are created on managed units cannot be seen or used.

For more information about creating a datasource in the cloud, see [create_cloud_datasource](#).

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

POST https://[Guardium hostname or IP address]:8443/restAPI/datasource

GuardAPI syntax

create_datasource parameter=value

Parameters

| Parameter | Value type | Description |
|-----------------------------|------------|--|
| application | String | Required. For valid values, call create_datasource from the command line with --help=true. |
| awsSecretsManagerConfigName | String | For Amazon Web Services (AWS) systems only. This parameter is needed when authentication is externally managed by the AWS secrets manager.
For valid values, call create_datasource from the command line with --help=true. |
| compatibilityMode | String | Valid values: <ul style="list-style-type: none">• Default• MSSQL 2000
Set the compatibility mode to use when monitoring a table. |
| conProperty | String | Define conProperty if additional connection properties are needed on the JDBC URL to establish a JDBC connection with this datasource.
For a Sybase database with a default character set of Roman8, enter the following property: charset=utf8 |
| customProps | String | |
| customURL | String | Define the connection string to the datasource. By default, the connection is made using host, port, instance, and other defined datasource parameters. This is useful, for example, when creating Oracle Internet Directory (OID) connections. |
| cyberarkConfigName | String | The name of the CyberArk configuration on your Guardium system. For valid values, call create_datasource from the command line with --help=true. |
| cyberarkObjectName | String | The CyberArk object name for the Guardium datasource. |
| dbInstanceAccount | String | Database account login name used by CAS. |
| dbInstanceDirectory | String | Directory where database software is installed that will be used by CAS. |
| dbName | String | The schema name for a Db2 or Oracle database. Otherwise, provide the database name. |
| description | String | Description of the datasource. |
| externalPasswordType | String | For valid values, call create_datasource from the command line with --help=true. |
| hashicorpChildNamespace | String | |
| hashicorpConfigName | String | The name of the HashiCorp configuration on your Guardium® system. For valid values, call create_datasource from the command line with --help=true. |
| hashicorpPath | String | The custom path to access the datasource credentials. |
| hashicorpRole | String | The role name for the datasource. |
| host | String | Host name or IP address of the database. |
| importServerSSLcert | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| KerberosConfigName | String | Name of the Kerberos configuration already defined in the Guardium system. |
| name | String | Required.
A unique name for the datasource on the Guardium system. |
| password | String | Database user password. |
| port | Integer | Database port number. |
| region | String | For AWS only. For valid values, call create_datasource from the command line with --help=true. |
| savePassword | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true)
Default = 1 (true)

Save and encrypt database authentication credentials on the Guardium system. This is required if you are defining a datasource with an application that runs as a scheduled task, for example scheduled classification scans. When enabled, name and password parameters are required. |
| secretName | String | |
| serviceName | String | Required for Oracle, Informix, Db2, and IBM i. For a Db2 database, provide the database name. Otherwise, provide the service name. |
| severity | String | Severity classification (or impact level) for the datasource.
For valid values, call create_datasource from the command line with --help=true. |

| Parameter | Value type | Description |
|---------------------|------------|--|
| shared | String | <p>Valid values:</p> <ul style="list-style-type: none"> • <i>Shared</i>: share the datasource with other applications • <i>Not Shared</i> • <i>true</i>: share the datasource with other applications • <i>false</i> <p>To share the datasource with other users, assign roles from the GUI.</p> |
| type | String | Required. The type of datasource. For valid values, call <code>create_datasource</code> from the command line with <code>--help=true</code> . |
| useExternalPassword | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • <i>0</i> (false) • <i>1</i> (true) |
| useKerberos | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • <i>0</i> (false) • <i>1</i> (true) <p>Enable to use Kerberos authentication. If enabled, <code>KerberosConfigName</code> is required.</p> |
| useLDAP | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • <i>0</i> (false) • <i>1</i> (true) <p>Enable to use LDAP.</p> |
| user | String | Database user name. If defined, password is required. |
| useSSL | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • <i>0</i> (false) • <i>1</i> (true) <p>Enable to use SSL authentication.</p> |
| walletZip | String | |

Examples

```
grdapi create_datasource type=DB2 name=chickenDB2 password=guardium user=db2inst1 dbName=dn0chick application=Access_policy
shared=true port=50000 host=chicken.corp.com
```

create_datasourceRef_by_id

This command creates a datasource reference for a specific object of a specific application type. The datasource, object, and application type are referenced by identification keys.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/datasource_ref_by_id
```

GuardAPI syntax

```
create_datasourceRef_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------|------------|--|
| appId | Integer | <p>Required. Identifies the application type.
Valid values:</p> <ul style="list-style-type: none"> • 8 (security assessment) • 47 (custom tables) • 51 (classifier) |
| dataSourceId | Integer | Required. Identifies the datasource by its identification key. |
| objId | Integer | Required. Identifies an instance of the specified appId type. For example, if <code>appId=51</code> , <code>objId</code> is the identification key of a classification process. |

Examples

```
grdapi create_datasourceRef_by_id appId=51 dataSourceId=20000 objId=2
```

create_datasourceRef_by_name

This command creates a datasource reference for a specific object of a specific application type. The datasource, object, and application type are referenced by name.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/datasource_ref_by_name
```

GuardAPI syntax

```
create_datasourceRef_by_name parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|--|
| application | String | Required. Identifies the application type. For valid values, call <code>create_datasourceRef_by_name</code> from the command line with <code>--help=true</code> . |
| datasourceName | String | Required. Identifies the datasource by its name. |
| objName | String | Required. Identifies an instance of the specified application type. For example, if <code>application=Classifier</code> , <code>objName</code> is the name of a specific classification process. |

Examples

```
grdapi create_datasourceRef_by_name application=Classifier datasourceName=swanSybase objName="class process1"
```

create_datasource_custom_property

This command defines a custom property for your datasource.

This API is available in Guardium V11.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/datasource_custom_prop
```

GuardAPI syntax

```
create_datasource_custom_property parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| name | String | Required. |
| values | String | Required. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Example

The following command creates the custom property called "Business Unit". "Retail", "Banking", "Consulting", and "Mortgage" are the associated values.

```
grdapi create_datasource_custom_property name="Business Unit" values="Retail, Banking, Consulting, Mortgage"
```

Related concepts

- [Datasource APIs](#)
-

create_datasource_group

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/datasource_group
```

GuardAPI syntax

```
create_datasource_group parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------------|------------|--|
| appTypeCriteria | String | For valid values, call <code>create_datasource_group</code> from the command line with <code>--help=true</code> . |
| customPropsCriteria | String | A list of datasource custom properties on which to filter datasources that belong to the group. |
| dbTypeCriteria | String | For valid values, call <code>create_datasource_group</code> from the command line with <code>--help=true</code> . |
| groupName | String | Required. The name of the group. |
| groupType | String | Required. Valid values: <ul style="list-style-type: none">• <i>DYNAMIC</i>• <i>STATIC</i> |
| hostCriteria | String | Host name criteria on which to filter datasources for this group. |
| severityCriteria | String | Valid values: <ul style="list-style-type: none">• <i>ALL</i>• <i>INFO</i>• <i>NONE</i>• <i>LOW</i>• <i>MED</i>• <i>HIGH</i> |
| userCriteria | String | User name criteria on which to filter datasources for this group. |

create_datasource_groupRef_by_id

Create datasource groups in security assessments, discovery scenarios, or custom tables.

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/datasource_group_ref
```

GuardAPI syntax

```
create_datasource_groupRef_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------|------------|--|
| appId | Integer | Required. For valid values, call <code>create_datasource_groupRef_by_id</code> from the command line with <code>--help=true</code> . |
| datasourceGroupId | Integer | Required. The datasource group ID in the <code>DATASOURCE_GROUP</code> table. |
| objId | Integer | Required. The object ID of the security assessment, discovery scenario, or custom table. |

create_datasource_groupRef_by_name

Create datasource groups in security assessments, discovery scenarios, or custom tables.

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/datasource_group_ref
```

GuardAPI syntax

```
create_datasource_groupRef_by_name parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------------|------------|--|
| application | String | Required. For valid values, call <code>create_datasource_groupRef_by_name</code> from the command line with <code>--help=true</code> . |
| datasourceGroupName | String | Required. The name of the datasource group. |
| objName | String | Required. The object ID of the security assessment, discovery scenario, or custom table. |

create_db_user_mapping

This command helps maintain the mapping between database users (that is, invokers of SQL that causes a violation) and email addresses for real-time alerts.

You can use wildcards as follows:

- `serverIp`: You can use the percent sign (%) as a wildcard instead of the character for any element in the IP address. For example, the following addresses are valid:
 - 192.168.2.%
 - 2620:1f7:807:%:920:%However, the following example is not valid: 192.%
- `serviceName`: Wildcards (%) are allowed.
- `dbUserName`: Wildcards are not valid. The % sign is not a special character.
- `emailAddress`: Wildcards are not valid. The % sign is not a special character.

Note: For `delete_db_user_mapping` and `list_db_user_mapping`, you can use the % wildcard for all parameters.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/db_user_mapping
```

GuardAPI syntax

```
create_db_user_mapping parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| dbUserName | String | Required. The DB username. |
| emailAddress | String | Required. For real-time alerts, the email address that maps to the DB user. The at symbol (@) is required. |
| serverIp | String | Required. The server IP address. |
| serviceName | String | Required. The server name. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GuardAPI example

```
grdapi create_db_user_mapping serverIp=192.168.1.% serviceName=ora1 dbUserName=hadrian emailAddress=hadrian.swall@company.com
```

Related concepts

- [Alerting rule actions](#)

Related reference

- [delete_db_user_mapping](#)
- [list_db_user_mapping](#)

create_ef_mapping

This command creates an external feed mapping and populates tables based on a specified report.

Each mapping has a name stored in EF_MAP_TYPE_HDR.EF_TYPE_DESC, and that name is identical to the value of the reportName parameter. The target table name is also based on the reportName parameter, with underscores added between the words. For example, the report *My Report* becomes *MY_REPORT*.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/create_ef_mapping
```

GuardAPI syntax

```
create_ef_mapping parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| reportName | String | Required. Name of the report to use for external feed mapping. This parameter also determines the name of the mapping and the target table name. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Use this command to create a mapping for the *Sessions per Day* report:

```
grdapi create_ef_mapping reportName="Sessions per Day"
```

create_entry_location

This command adds an archive catalog entry to the catalog location table.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/entry_location
```

GuardAPI syntax

```
create_entry_location parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| entryType | String | Required. The type of archive file. Valid values: <ul style="list-style-type: none">• CollectorDataArchive• AggDataArchive• AggResultArchive |
| fileName | String | Required. The name of the archive file in one of these formats: <ul style="list-style-type: none">• <day of data>-<Guardium system name>-w<time of zip>-d<execution date>.dbdump.enc• <day of data>-<Guardium system name>-w<time of zip>-d<execution date>.agg.<sql ver>.tar.gc.enc |
| hostName | String | Required. The hostname or IP address. |
| password | String | The user's password. <ul style="list-style-type: none">• Amazon S3: Secret Access Key• IBM COS: Secret Access Key• IBM Cloud: X-Auth-Key |
| path | String | Required. The path to the archive directory. <ul style="list-style-type: none">• Amazon S3: bucket name• IBM COS: bucket name• EMC Centera: Centera clipID• FTP: Specify the directory relative to the FTP account home directory.• SCP: Specify the directory as an absolute path.• IBM Cloud: Container• TSM: path |
| processDesc | String | Required when the entryType = AggResultArchive. |
| retention | Integer | The number of days to keep the entry in the catalog.
Default = 365 |
| storageSystem | String | Required. The type of archive storage system. For valid values, call create_entry_location from the command line with --help=true . |
| user | String | The user account to access the host. <ul style="list-style-type: none">• Amazon S3, Cleversafe: Access Key ID• Softlayer: X-Auth-User <p>Attention: For storageSystem type FTP, the user value cannot include any of the following characters: ! " \$ & ' () ; \ </p> |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI Example

```
grdapic create_entry_location entryType=CollectorDataArchive  
fileName=733392-a1.corp.com-w20071223.133546-d2007-12-27.dbdump.enc password=somePassword  
user=someUser path=/var/dump/ hostName=192.168.1.241 storageSystem=scp
```

Related tasks

- [Data and Result catalogs](#)

Related reference

- [Archive, export, import, purge, and restore APIs](#)
- [Catalog entry APIs](#)

create_fam_rule

This command creates a FAM rule. Each rule defines a set of conditions, and an action that is taken by Guardium® when the rule matches.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/famPolicyRule
```

GuardAPI syntax

```
create_fam_rule parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------------|------------|---|
| actionName | String | Required. The action taken when the rule criteria are met. Valid values: <ul style="list-style-type: none">• <i>Alert and audit</i>: Send an alert directly generated from the sniffer with specific behavior, and log the event.• <i>Audit only</i>: Log the event in GDM tables• <i>Block, log violation, and audit</i>: Block access to the object, log a policy violation, and log the event. A blocking action requires an alert configuration as well.• <i>Ignore</i>: No action taken.• <i>Log as violation and audit</i>: Log this as a policy violation and log the event. |
| alertReceiver | String | Recipient of the alert: any user of the appliance, for example admin. |
| classDestination | String | Name of the custom class to be invoked. For valid values, call <code>create_fam_rule</code> from the command line with <code>--help=true</code> . |
| command | String | The command name to be matched. If not specified, all file system commands are counted as a match. For valid values, call <code>create_fam_rule</code> from the command line with <code>--help=true</code> . |
| commandGroup | String | Name of the group of commands to be matched. Either <code>commandGroup</code> or <code>commandGroupId</code> must be specified. |
| commandGroupId | Integer | ID of the group of commands to be matched. Either <code>commandGroup</code> or <code>commandGroupId</code> must be specified. |
| filePath | String | File path to be monitored, or excluded from monitoring. See <code>notfilePath</code> . Either <code>filePath</code> or <code>filePathGroup</code> must be specified. |
| filePathGroup | String | Group of file paths to be monitored, or excluded from monitoring. See <code>notfilePath</code> . Either <code>filePath</code> or <code>filePathGroup</code> must be specified. |
| includeSubDirectory | String | Required. Whether or not files in subdirectories are included or not. Valid values: <ul style="list-style-type: none">• <i>yes</i>: include files in all subdirectories• <i>no</i>: do not include files in subdirectories |
| messageTemplate | String | Message template name. For valid values, call <code>create_fam_rule</code> from the command line with <code>--help=true</code> . |
| notfilePath | String | Required. Valid values: <ul style="list-style-type: none">• <i>yes</i>: apply this rule to all files except those in the specified path, either <code>filePath</code> or <code>filePathGroup</code>• <i>no</i>: apply this rule to all files in the specified path, either <code>filePath</code> or <code>filePathGroup</code> |
| notificationType | String | Notification type. Valid values: <ul style="list-style-type: none">• <i>MAIL</i>• <i>SNMP</i>• <i>CUSTOM</i>• <i>SYSLOG</i> |
| notOSUser | String | Required. Valid values: <ul style="list-style-type: none">• <i>yes</i>: evaluate this FAM rule for all users except the specified <code>osUser</code> or <code>osUserGroup</code>.• <i>no</i>: evaluate this FAM rule for all users. |
| osUser | String | The OS user to whom this rule applies. If <code>osUser</code> or <code>osUserGroup</code> are unspecified, then the rule applies to all users (except root). |
| osUserGroup | String | The group of OS user names to whom this rule applies. If <code>osUser</code> or <code>osUserGroup</code> are unspecified, then the rule applies to all users (except root). |
| policyName | String | Required. Name of policy to which this rule is added. For valid values, call <code>create_fam_rule</code> from the command line with <code>--help=true</code> . |
| removableMedia | String | Required. Include removable media when evaluating criteria. Valid values: <ul style="list-style-type: none">• <i>yes</i>• <i>no</i> |
| ruleName | String | Required. A unique rule name. |
| serverHost | String | Host name to monitor. Use <code>x.x.x.x</code> to monitor all servers. Either <code>serverHost</code> or <code>serverHostGroup</code> must be specified. |
| serverHostGroup | String | Guardium group of server hostnames to monitor. Either <code>serverHost</code> or <code>serverHostGroup</code> must be specified. |

Examples

```
grdapi create_fam_rule policyName=policy1 ruleName=rule1 serverHost="x.x.x.x" filePath="/famtest/*" command="DELETE"  
actionName="Alert and Audit" notificationType="SYSLOG"
```

Related concepts

- [FAM discovery and classification in Windows and UNIX-Linux file servers](#)
- [Using rules for file activity policies](#)

Related reference

- [delete_policy](#)
- [create_policy](#)
- [list_policy_fam_rule](#)
- [enable_fam_crawler](#)
- [disable_fam_crawler](#)
- [add_action_to_fam_rule](#)
- [get_fam_crawler_info](#)
- [policy_fam_rule_delete](#)

create_group

This command defines a group.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/group
```

GuardAPI syntax

```
create_group parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|--|
| appid | String | Required. For valid values, call <code>create_group</code> from the command line with <code>--help=true</code> . |
| category | String | A category is an optional label that is used to group policy violations and groups for reporting. |
| classification | String | A classification is an optional label that is used to group policy violations and groups for reporting. |
| desc | String | Required. Enter a unique description for the new group. |
| hierarchical | String | Valid values: <ul style="list-style-type: none">• <i>true</i>• <i>false</i> |
| tuple_parameters | String | Required. Valid values: <ul style="list-style-type: none">• <i>client_ip</i>• <i>client_host_name</i>• <i>server_ip</i>• <i>server_host_name</i>• <i>source_program</i>• <i>db_name</i>• <i>db_user</i>• <i>service_name</i>• <i>app_user_name</i>• <i>os_user</i>• <i>db_type</i>• <i>net_protocol</i>• <i>command</i>• <i>server_port</i>• <i>sender_ip</i>• <i>server_description</i>• <i>analyzed_client_ip</i>• <i>incident</i>• <i>session</i>• <i>client_os_name</i>• <i>server_os_name</i>• <i>db_prototype</i>• <i>field_name</i>• <i>error_code</i> |
| type | String | Required. For valid values, call <code>create_group</code> from the command line with <code>--help=true</code> . |

Examples

Use this command to create a *public OBJECTS* group named *A public group*:

```
grdapi create_group desc="A public group" type=OBJECTS appid=Public
```

create_hashicorp_config

This command creates a HashiCorp configuration on your Guardium® system.

This API is available in Guardium v11.4 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/hashicorp
```

GuardAPI syntax

```
create_hashicorp_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| AuthType | String | Required. For valid values, call <code>create_hashicorp_config</code> from the command line with <code>--help=true</code> . |
| name | String | Required. The name of the HashiCorp configuration. |
| namespace | String | |
| password | String | The username. |
| username | String | The password. |
| useTLS | Boolean | Transport Layer Security (TLS) with server-side or client-side authentication.
Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| vaultHostName | String | Required. The vault hostname. |
| vaultPortNumber | Integer | Required. The port number. |

Examples

This example creates a configuration with a username and password with no Transport Layer Security (TLS):

```
grdapi create_hashicorp_config AuthType="Username & Password" name="No TLS User and password API" username="apps" password="guardium" useTLS="false" vaultHostName="hostname" vaultPortNumber="8300"
```

This example creates a configuration with TLS server authentication:

```
grdapi create_hashicorp_config AuthType="Username & Password" name="TLS User and password API" username="apps" password="guardium" useTLS="true" vaultHostName="hostname" vaultPortNumber="8500"
```

This example creates a configuration with TLS client authentication. The username and password is not required:

```
grdapi create_hashicorp_config AuthType="TLS Certificates" name="TLS Client Cert API" useTLS="true" vaultHostName="hostname" vaultPortNumber="8200"
```

Related concepts

- [Datasource credential management APIs](#)

create_hierarchical_member_to_group_by_desc

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/hierarchical_member
```

GuardAPI syntax

```
create_hierarchical_member_to_group_by_desc parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| desc | String | Required. |
| member | String | Required. |

create_kafka_cluster

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/kafka_cluster
```

GuardAPI syntax

```
create_kafka_cluster parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|---|
| clusterName | String | Required. |
| memberList | String | Required
For valid values, call create_kafka_cluster from the command line with --help=true. |

create_member_to_group_DAMX_Standard_Activity

This API is available in Guardium V10.1.4 and later.

GuardAPI syntax

```
create_member_to_group_DAMX_Standard_Activity parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| member | String | Required. |

create_member_to_group_DAMX_Suspicious_Connections

This API is available in Guardium V10.1.4 and later.

GuardAPI syntax

```
create_member_to_group_DAMX_Suspicious_Connections parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| member | String | Required. |

create_member_to_group_by_desc

Add a member to a group identified by its description.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/group_member
```

GuardAPI syntax

```
create_member_to_group_by_desc parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| desc | String | Required. Identifies the group by its description. |
| member | String | Required. The group member name, which must be unique within the group. The group member name might be a tuple, that is, a single composite group member formed of multiple attributes. For more information, see Tuple groups . |

Examples

Use this command to add the group member *turkey* to the group "A group":

```
grdapi create_member_to_group_by_desc desc="A group" member=turkey
```

Use this command to add a group member to the group "A group". For this group, a 5-tuple member is required:

```
grdapi create_member_to_group_by_desc desc="A group" member=10.0.1.1+SrcApp+DBUser2+%+SvcName+OSUser2+%
```

Related concepts

- [Groups Overview](#)

create_member_to_group_by_id

Add a member to a group identified by its identification key.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/group_member_by_group_id
```

GuardAPI syntax

```
create_member_to_group_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| id | Integer | Required. Identifies the group by its identification key. |
| member | String | Required. The group member name, which must be unique within the group. The group member name might be a tuple, that is, a single composite group member formed of multiple attributes. For more information, see Tuple groups . |

Examples

Use this command to add the group member *turkey* to the group with identification key *100005*:

```
grdapi create_member_to_group_by_id id=100005 member=turkey
```

Use this command to add a group member to the group with identification key *100005*. For this group, a 5-tuple member is required:

```
grdapi create_member_to_group_by_id id=100005 member=10.0.1.1+SrcApp+DBUser2+%+SvcName+OSUser2+%
```

Related concepts

- [Groups overview](#)

create_online_report

This command creates an ad hoc online report in JSON format.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available only as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/online_report
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| reportName | String | Required. For valid values, call <code>create_online_report</code> from the command line with <code>--help=true</code> . |
| indexFrom | Integer | |
| inputTZ | String | For valid values, call <code>create_online_report</code> from the command line with <code>--help=true</code> . |
| reportParameter | String | |
| fetchSize | Integer | |
| sortColumn | String | |
| sortType | String | |
| showAll | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| showIndirect | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |

Example

The following example creates an online Installed Policy Details report to find the currently installed policy:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/online_report \
{"reportName":"Installed Policy Details","indexFrom":"1", \
"reportParameter": {""QUERY_FROM_DATE" :"NOW -1 DAY", \
"QUERY_TO_DATE" :"NOW +1 HOUR", "REMOTE_SOURCE": "%"}}
```

Related reference

- [Reporting and report generation APIs](#)
-

create_policy

This command creates a new policy.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/policy
```

GuardAPI syntax

```
create_policy parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------|------------|--|
| baselineDesc | String | |
| categoryName | String | An existing data or file policy. For valid values, call <code>create_policy</code> from the command line with <code>--help=true</code> . |

isFam

Boolean

Determines whether this policy is for file access monitoring. Valid values:

- 0 (false): This is a data access monitoring policy.
- 1 (true): This is a file access monitoring policy.

Default = 0 (false)

For more information, see [Using rules for file activity policies](#).

| Parameter | Value type | Description |
|-----------------|------------|---|
| logFlat | Boolean | Determine whether to use the flat log option for this policy. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false)
For more information, see Log flat . |
| pattern | String | A regular expression to match. For more information, see Pattern in Rule definition fields . |
| policyLevel | String | Valid values: <ul style="list-style-type: none">• REGULAR• SESSION• FAM• FAM_SP• FAM_NAS• 0• 1• 2• 3• 4 Default = REGULAR |
| ruleSetDesc | String | Required. The name of this policy. |
| rulesOnFlat | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false)
For more information, see Rules on flat . |
| securityPolicy | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

create_qr_action

This command creates a query rewrite action for a specified query rewrite definition.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/qr_action
```

GuardAPI syntax

```
create_qr_action parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|---|
| actionName | String | Required. The unique name of the query rewrite action. |
| definitionName | String | Required. The query rewrite definition that is associated with this action. |
| description | String | Text description of the action. |

Examples

To create a query rewrite action "qr action15_3" associated with the definition "case 15":

```
grdapicreate_qr_action definitionName="case 15" actionPerformed="qr action15_3"
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

create_qr_add_where

This command associates a query rewrite function to add a WHERE condition to the specified query rewrite action.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/qr_add_where
```

GuardAPI syntax

```
create_qr_add_where parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|---|
| actionName | String | Required. The unique name of the query rewrite action. |
| addQualifierFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0(false)• 1(true) Default = 1 (true) |
| definitionName | String | Required. The query rewrite definition that is associated with this action. |
| whereText | String | Text to add to a WHERE clause. |

Examples

To add a WHERE clause of "id=2" to the query rewrite definition "qrw_def_Oracle_1" and action name "qrw_act__addwhere_id2":

```
grdapicreate_qr_add_where definitionName="qrw_def_Oracle_1" actionPerformed="qrw_act__addwhere_id2" whereText="id=2"
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

create_qr_add_where_by_id

This command associates a query rewrite function to add a WHERE condition to the specified query rewrite action, where the action is specified by its ID.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/create_qr_add_where_by_id
```

GuardAPI syntax

```
create_qr_add_where_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|---|
| addQualifierFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0(false)• 1(true) Default = 1 (true) |
| qrActionId | Long | Required. The unique ID of query rewrite action. |
| whereText | String | Text to add to a WHERE clause. |

Examples

To add a WHERE clause of id=2 to the action whose ID is 10002:

```
grdapi create_qr_add_where_by_id qrActionId=10002 whereText="id=2"
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

create_qr_condition

This command creates a query rewrite condition.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/qr_condition
```

GuardAPI syntax

```
create_qr_condition parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------------|------------|--|
| conditionName | String | Required. The unique name of this query rewrite condition. |
| definitionName | String | Required. The query rewrite definition that is associated with this condition. |
| depth | Integer | Integer that specifies the depth of the parsed SQL that this condition applies to (1 and higher). The default -1 means that the query rewrite condition applies to any matching SQL at any depth. |
| isForAllRuleObjects | Boolean | Use this parameter to associate this condition with objects in a policy access rule. The default is false, which means neither option impacts any rule triggering behavior. Valid values: <ul style="list-style-type: none">• 0: False. the query condition is specified using the objects that are defined in this condition.• 1: True. The specified condition applies to all objects in the access rule's Object field or Object group for a fired rule. |
| isForAllRuleVerbs | Boolean | Use this parameter to associate this condition with objects in a policy access rule. The default is false, which means neither option impacts any rule triggering behavior. Valid values: <ul style="list-style-type: none">• 0: False. The query condition is specified using the verbs that are defined in this condition.• 1: True. The specified condition applies to all verbs in the access rule's Verb field or Verb group for a fired rule. |
| isObjectRegex | Boolean | Indicates that the specified object is specified by using a regular expression. Default is false. Valid values: <ul style="list-style-type: none">• 0: False• 1: True |

| Parameter | Value type | Description |
|-------------|------------|--|
| isVerbRegex | Boolean | Indicates that the specified verb is specified by using a regular expression. Default is false. Valid values: <ul style="list-style-type: none">• 0: False• 1: True |
| object | String | An object (table, view). The default "*" means all objects. This can also be specified as a regular expression, in which case set the isVerbRegex to True. |
| order | Integer | Specifies the order in which to assemble multiple related query rewrite conditions for complex SQL. Default is 1. |
| verb | String | A verb (select, insert, update, delete). The default "*" means all verbs. |

Examples

To create a query rewrite condition with the definition name "case 15" and condition name qr cond15_3, the verb SELECT, valid for any object, parsed down 2 levels:

```
grdapicreate_qr_condition definitionName="case 15" conditionName="qr cond15_3" verb=select object=* depth=2
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

create_qr_definition

This command creates a query rewrite definition.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/qr_definition
```

GuardAPI syntax

```
create_qr_definition parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|--|
| dataBaseType | String | Required. The type of database this query rewrite definition is associated with. For valid values, call create_qr_definition from the command line with --help=true . |
| definitionName | String | Required. A unique name for this query rewrite definition condition. |
| description | String | Textual description. |
| isNegateQrCond | Boolean | Specifies if there is a NOT flag on the set of query rewrite conditions that are associated with this definition. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| sampleSql | String | |

Examples

To create a query rewrite condition named case 15, for Oracle databases:

```
grdapicreate_qr_definition dataBaseType="ORACLE" definitionName="case 15"
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

create_qr_replace_element

This command creates a replacement element, or set of elements, such as an entire SQL sentence or a SELECT list.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/qr_replace_element
```

GuardAPI syntax

```
create_qr_replace_element parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|--|
| actionName | String | Required. The unique name of the query rewrite action this rewrite function is associated with. |
| columnAlias | String | Specify an alias for a column name. |
| definitionName | String | Required. A unique name for this query rewrite definition condition. |
| isFromAllRuleElements | Boolean | Indicates that this action applies to all FROM elements. Valid values: <ul style="list-style-type: none">• 0: False• 1: True Default is false. |
| isFromRegex | Boolean | Indicates that the 'from' element is specified by using a regular expression. Valid values: <ul style="list-style-type: none">• 0: False• 1: True Default is false. |
| isReplaceToFunction | Boolean | Indicates that the "replace to" is the name of a function, such as user-defined function. Valid values: <ul style="list-style-type: none">• 0: False• 1: True |
| replaceFrom | String | Required. The incoming string for a matching rule that is to be replaced. Use replaceType to indicate specifically which element of the incoming query to examine. |
| replaceTo | String | Required. The replacement string for the matching element. |
| replaceType | String | Required. Indicates what is to be replaced. For valid values, call create_qr_replace_element from the command line with --help=true. |

Examples

```
grdapi create_qr_replace_element definitionName="case 15" actionName="qr_action15_2" replaceType=VERB replaceFrom="select" replaceTo="select++"
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

create_qr_replace_element_byId

This command creates a replacement specification for a specified query rewrite action.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/create_qr_replace_element_byId
```

GuardAPI syntax

```
create_qr_replace_element_byId parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|--|
| columnAlias | String | Specify an alias for a column name. |
| isFromAllRuleElements | Boolean | Indicates that this action applies to all FROM elements. Valid values: <ul style="list-style-type: none">• 0: False• 1: True Default is false. |
| isFromRegex | Boolean | Indicates that the "from" element is specified by using a regular expression. Valid values: <ul style="list-style-type: none">• 0: False• 1: True Default is false. |
| isReplaceToFunction | Boolean | Indicates that the "replace to" is the name of a function, such as user-defined function. Valid values: <ul style="list-style-type: none">• 0: False• 1: True |
| qrActionId | Long | Required. The unique ID of query rewrite action. |
| replaceFrom | String | Required. The incoming string for a matching rule that is to be replaced. Use replaceType to indicate specifically which element of the incoming query to examine. |
| replaceTo | String | Required. The replacement string for the matching element. |
| replaceType | String | Required. Indicates what is to be replaced. For valid values, call create_qr_replace_element_byId from the command line with --help=true. |

Examples

```
grdapicreate_qr_replace_element_byId qrActionID="1116" replaceType=OBJECT replaceFrom="employee" replaceTo="employee_2"
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

create_quarantine_allowed_until

This command sets parameters to prevent a user from logging in after a specified length of time passes.

This API is available in Guardium® V9.5 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/quarantine_allowed_until
```

GuardAPI syntax

```
create_quarantine_allowed_until parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------|------------|--|
| allowedUntil | String | Required. The date and time to begin the quarantine in one of the following formats: <ul style="list-style-type: none">• YYYY-MM-DD hh:mm:ss• A relative time (such as NOW +1 HOUR) For more information about relative time, see Relative to NOW . |
| dbUser | String | Required. The name of the database user to quarantine. |
| serverIp | String | Required. The server IP address. |
| serviceName | String | Required. The server name. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| type | String | Required. If the database is not IBM Z® or IMS, specify <i>normal</i> . Valid values: <ul style="list-style-type: none">• <i>normal</i>• <i>DB2Z</i>• <i>IMS</i> |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• <i>all_managed</i>: execute on all managed units but not the central manager• <i>all</i>: execute on all managed units and the central manager• <i>group:<group name></i>: execute on all managed units identified by <i><group name></i>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GuardAPI example

The following command starts the quarantine for this user to start 1 hour after the command is called:

```
grdapi create_quarantine_allowed_until allowedUntil="NOW +1 HOUR" dbUser="Hadrian.Swall" serverIp="9.32.0.255" serviceName="company.ibm.com" type="normal"
```

Related concepts

- [Dates and Timestamps](#)
- [Logging or ignoring rule actions](#)

create_quarantine_until

This command sets parameters to prevent a user from logging in until a specified time.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/quarantine_until
```

GuardAPI syntax

```
create_quarantine_until parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| dbUser | String | Required. The name of the database user to quarantine. |
| quarantineUntil | String | Required. The date and time to end the quarantine in one of the following formats: <ul style="list-style-type: none">• YYY-MM-DD hh:mm:ss• A relative time (such as NOW +1 HOUR) For more information about relative time, see Relative to NOW . |
| serverIp | String | Required. The server IP address. |
| serviceName | String | Required. The server name. |
| type | String | Required. If the database is not IBM Z® or IMS, specify <i>normal</i> . Valid values: <ul style="list-style-type: none">• <i>normal</i>• <i>DB2Z</i>• <i>IMS</i> |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

The following command ends the quarantine for this user 1 hour after the command is called:

```
grdapi create_quarantine_until quarantineUntil="NOW +1 HOUR" dbUser="Hadrian.Swall" serverIp="9.32.0.255"
serviceName="company.ibm.com" type="normal"
```

Related concepts

- [Dates and Timestamps](#)
- [Logging or ignoring rule actions](#)

create_role

This command creates a role on a stand-alone or central manager system.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/create_role
```

GuardAPI syntax

```
create_role parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| roleName | String | Required. |

GuardAPI example

```
grdapi create_role roleName test_role
```

Related concepts

- [Understanding roles](#)

create_rule

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/rule
```

GuardAPI syntax

```
create_rule parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| category | String | For valid values, call create_rule from the command line with --help=true. |
| classification | String | |
| fromPolicy | String | Required. |
| order | Integer | |
| ruleDesc | String | Required. |
| ruleLevel | String | |
| ruleType | String | Required. For valid values, call create_rule from the command line with --help=true. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

create_rule_action

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/rule_action
```

GuardAPI syntax

```
create_rule_action parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------------|------------|-------------|
| actionLevel | String | |
| actionName | String | Required. |
| actionParameters | String | |
| alertUserLoginName | String | |
| classDestination | String | |
| fromPolicy | String | Required. |
| messageTemplate | String | |
| notificationType | String | |
| paramSeparator | String | |
| ruleDesc | String | Required. |

create_sql_configuration

This command defines the connection between an S-TAP® and an Oracle server used for Oracle unified auditing.

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/create_sql_configuration
```

GuardAPI syntax

```
create_sql_configuration parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|---|
| dbType | String | Required. The type of data repository being monitored. Valid value: <ul style="list-style-type: none">• Oracle |
| instance | String | Required. String that specifies the connection identifier in the tnsnames.ora that is used to connect to the database. |
| dataPullInterval | String | Time, in seconds, between attempts to pull data from the database.
Default=30 |
| dataPullRows | String | Number of rows of auditing data to pull in a single pass.
Default=100 |
| stapHost | String | Required. For valid values, call create_sql_configuration from the command line with --help=true. |
| timeout | String | Time, in seconds, to allow the database to respond.
Default=300000 |
| username | String | Required. Username for logging in to the Oracle DB. |
| userRole | String | Role for logging in to the Oracle DB. Valid values <ul style="list-style-type: none">• ''• sysdba• sysoper Default = '' |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

create_stap_inspection_engine

This command adds an inspection engine to the specified S-TAP®. S-TAP configurations can be modified only from the active Guardium® host for that S-TAP, and only when the S-TAP is online.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/inspection_engine
```

GuardAPI syntax

```
create_stap_inspection_engine parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------------|------------|---|
| client | String | Restricts S-TAP to monitor traffic only from the specified sets of IP address and mask pairs, by using a list of addresses in IP address/mask format: n.n.n.n/m.m.m.m. If an improper IP address/mask is entered, the S-TAP does not start. Valid values: <ul style="list-style-type: none">• User-defined list• 0.0.0.0/0.0.0.0,::/0: select all clients.• 127.0.0.1/255.255.255.255,::1/0: local traffic only Client Ip/Mask (networks) and Exclude Client Ip/Mask (exclude networks) cannot be specified simultaneously. If the value of this parameter is not configured correctly, the value is replaced by the default value. |
| connectToIp | String | IP address for S-TAP to use to connect to the database. Some databases accept local connection only on the real IP address of the Guardium system, and not on the default (127.0.0.1,::1). When K-TAP is enabled, this parameter is used for Solaris zones and AIX® WPARs. Set it to the zone IP address to capture traffic. |
| db2SharedMemAdjustment | Integer | Required when Db2® is selected as the database type, and shared memory connections are monitored. The offset to the server's portion of the shared memory area. Offset to the beginning of the Db2 shared memory packet, depends on the Db2 version: 32 in pre-8.2.1, and 80 in 8.2.1 and higher. |

| Parameter | Value type | Description |
|--|------------|---|
| db2SharedMemClientPosition (DB2® only) | Integer | <p>The offset to the client's portion of the shared memory area. Required when Db2 is selected as the database type, and shared memory connections are monitored. Linux: Use the script <code>find_db2_shmem_parameters.sh</code> to find the value. The script is located in <code>stap_directory/bin</code>, and outputs what the Db2 shared memory parameters that are defined in the Inspection Engines should be. Run it either as root or Db2 user, by using the syntax: <code>find_db2_shmem_parameters.sh <instance name></code>. You can run it from any directory.</p> <p>Windows: The client offset can be calculated by taking the value of the Db2 parameter ASLHEAPSZ and multiplying by 4096 to get the appropriate offset. The default for this parameter is 61440 decimal. This parameter is calculated by taking the Db2 database configuration value of ASLHEAPSZ and multiplying by 4096. To get the value for ASLHEAPSZ, run <code>runexec</code> the following Db2 command: <code>db2 get dbm cfg</code> and look for the value of ASLHEAPSZ. This value is typically 15, which yields the 61440 default. If it's not 15, take the value and multiply by 4096 to get the appropriate client offset.</p> |
| db2SharedMemSize | Integer | Db2 shared memory segment size. Required when Db2 is selected as the database type, and shared memory connections are monitored. |
| dbInstallDir (Linux only) | String | <ul style="list-style-type: none"> Db2, Informix®: The full path name for the database installation directory. Db2 exit and Informix exit: value must be the same as the \$HOME value in the database (or \$Db2_HOME for Db2 Exit); otherwise tap_identifier does not function properly. Oracle: Database owner HOME directory. It must match db_base in the ATAP configuration. See Oracle-specific guardctl parameters. All other database types: NULL. |
| dbUser | String | OS username (case-sensitive) of the owner of the DB server process (for example, oracle). This parameter specifies which user is allowed to use the db_request_handler socket. It is required if you are not using the user root. If set to an invalid value, A-TAP cannot access the socket to retrieve permission for accessing K-TAP. In this case, it requires authorization with a group membership to log decrypted traffic to K-TAP (by using the <code>guardctl authorize-user</code> command). You can define a comma-separated string of multiple users. |
| dbVersion | String | The database version. The string must start with a numeral and not a letter. |
| encryption (Linux only) | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> 0: Unencrypted 1: Encrypted <p>Default = 0 (false)</p> <p>Activate ASO or SSL encrypted traffic for Oracle (versions 11 and 12) and Sybase on Solaris, HPUX, and AIX.</p> <p>For Oracle, specify db_version in the <code>guard_tap.ini</code> file (for example, <code>db_version=12</code>)</p> <p>For Oracle12 SSL, instrument on all platforms. For Oracle11 SSL, instrument on AIX.</p> <p>For any Oracle requiring instrumentation, if you are using encryption=1 in the <code>guard_tap.ini</code> (which is not supported on Linux®), you must instrument before setting that parameter.</p> <p>Some DBs require restart after enabling encryption.</p> <p>When using GIM to configure the S-TAP, <code>GIM_ROOT_DIR</code> must be set to the absolute path to the modules, for example <code>/usr/local/guardium/modules</code></p> |
| excludeClient | String | A list of client IP addresses and corresponding masks that are excluded from monitoring. Use this option to configure the S-TAP to monitor all clients, except for a certain client or subnet (or a collection thereof). Client Ip/Mask (networks) and Exclude Client Ip/Mask (exclude networks) cannot be specified simultaneously. |
| ieIdentifier | String | Used to distinguish inspection engines from one another. If unspecified, Guardium auto-populates the field with a unique name that uses the database type and sequence number. |
| informixVersion | Integer | Informix version. |
| instanceName (Windows only) | String | The name of the database instance on this server. Required for MS SQL Server that uses encryption; MS SQL Server that uses Kerberos Authentication; Db2 Exit traffic collection; Db2 SHM traffic. (Default is MSSQLSERVER.) |
| interceptTypes (Linux only) | String | DO NOT change this parameter unless it is absolutely necessary. Protocol types that are intercepted by the IE. Valid values: <ul style="list-style-type: none"> NULL: auto intercepts all protocols the Database supports Comma-separated list: IE intercepts these protocol types only. |
| ktapDbPort (Linux only) | String | With K-TAP and PCAP, identifies the database port or range of ports to be monitored. For exit libraries, use its value for db_home. |
| namedPipe (Windows only) | String | Specifies the named pipe that is used by MS SQL Server local access. If a named pipe is used, but nothing is specified in this parameter, S-TAP attempts to retrieve the named pipe name from the registry. |
| portMax | String | For monitoring network traffic only, the highest numbered port on which to listen for database traffic. |
| portMin | String | For monitoring network traffic only, the lowest numbered port on which to listen for database traffic. Together with portMax, this parameter defines the range of ports that are monitored for this database instance. Usually the range contains only a single port. For a Kerberos inspection engine, set the start and end values to 88-88. If a range is used, do not include extra ports in the range. Extra ports might result in excessive resource consumption while the S-TAP attempts to analyze unwanted traffic.
Examples:
To monitor range 1521-1525 (five ports) with no port forwarding: <ul style="list-style-type: none"> portMin=1521 portMax=1525 ktapDbPort=1521 To monitor range 2000-2004 (5 ports) where network port 2000 is mapped to local port 1521: <ul style="list-style-type: none"> portMin=2000 portMax=2004 ktapDbPort=1521 |

| Parameter | Value type | Description |
|------------------------------|------------|---|
| priorityCount | Integer | <p>Reduces the instances of a blank DB_USER or ? in the tables. At session creation, the first priority_count packets are marked with a high priority flag and are transferred to a special high priority queue on the collector. Valid values:</p> <ul style="list-style-type: none"> • 0: Disabled • Protocol 7: 1-2048: Number of packets • Protocol 8: positive integer: Number of packets <p>Default = 20</p> |
| procName (Linux only) | String | <p>The value of this parameter depends on whether it's in an exit, and whether there is A-TAP.</p> <ul style="list-style-type: none"> • Exit libraries: see Configuring Exit libraries • With A-TAP: see Database-specific guardctl parameters • Without A-TAP: The full path name for the database executable. For example: <ul style="list-style-type: none"> ◦ Oracle: /\$ORACLE_HOME/bin/oracle ◦ Informix: /INFORMIXTMP/.inf.sqlexec. Applies to all Informix platforms but Linux. ◦ Informix with Linux, example: /home/informix11/bin/oninit ◦ MYSQL: mysql |
| procNames (Windows only) | String | Database service executables that are to be monitored. For example, a Db2 IE would be TAP_DB_PROCESS_NAMES=Db2SYSCS.EXE. For Oracle or MS SQL Server only, when named pipes are used. For Oracle, the list usually has two entries: oracle.exe,tnslsnr.exe. For MS SQL Server, the list is usually one entry: sqlservr.exe. |
| protocol | String | Required. The type of data repository that is monitored.
Linux-UNIX: ASTERDB, Cassandra, CockroachDB, CouchDB, Db2, Db2 Exit, ElasticSearch, exclude IE, FTP, GreenplumDB, HADOOP, HIVE, HP-Vertica, HTTP, HUE, IMPALA, Informix, Informix Exit, KERBEROS, MariaDB, MemSQL, MongoDB, Mysql, Netezza®, Oracle, PostgreSQL, REDIS, SAP Hana, Sybase, Teradata, Teradata Exit, WebHDFS, Windows File Share
Windows: ASTER, Cassandra, CouchDB, Db2, Db2 Exit, exclude IE, FTP, GreenplumDB, HIVE, HTTP, HUE, IMPALA, Informix, Informix Exit, MariaDB, MongoDB, MSSQL, Mysql, Oracle, PostgreSQL, Sybase, Teradata, WebHDFS, Windows File Share. |
| stapHost | String | Required. The host name or IP address of the database server on which the S-TAP is installed. |
| teeListenPort | String | Deprecated. Replaced by the parameter real_db_port when the K-TAP monitoring mechanism is used. |
| teeRealPort | String | Deprecated. |
| unixSocketMarker(Linux only) | String | Specifies UNIX domain sockets marker for Oracle, MySQL, and Postgres. Usually the default is correct, but when the named pipe or UNIX domain socket traffic does not work then you need to make sure that this value is set correctly. For example, for Oracle, set unix_domain_socket_marker to the KEY of IPC defined in tnsnames.ora. If it is NULL or not set, the S-TAP uses defined default markers identified as: * MySQL - "mysql.sock" * Oracle - "./oracle/" * Postgres - ".s.PGSQL.5432" |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To create an inspection engine on an MYSQL database with IP 127.0.0.1:

```
grdapicreate_stap_inspection_engine connectToIp=127.0.0.1 db2SharedMemAdjustment=80 db2SharedMemClientPosition=0
db2SharedMemSize=131072 procName=/home/mysql57/mysql/bin/mysql dbInstallDir=/home/mysql57 protocol=Mysql dbUser=mysql
encryption=0 dbVersion=9
```

Related concepts

- [Inspection engine configuration](#)

Related tasks

- [Linux-UNIX: Configuring an inspection engine](#)
- [Windows: Configuring an inspection engine](#)

Related reference

- [S-TAP and inspection engine APIs](#)

create_test_detail_exception

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/test_detail_exception
```

GuardAPI syntax

```
create_test_detail_exception parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------------|------------|--|
| assessmentDesc | String | |
| assessmentScope | String | |
| datasourceGroup | String | |
| datasourceName | String | |
| datasourceScope | String | |
| datasourceType | String | |
| detailExceptionValue | String | Required. |
| exceptionType | String | Required. Valid values: <ul style="list-style-type: none">• <i>text</i>• <i>regex</i>• <i>0</i>• <i>1</i> |
| explanation | String | Required. |
| fromDate | String | |
| testDescription | String | Required. |
| toDate | String | Required. |

create_test_exception

This command adds records to the vulnerability assessment test exceptions.

If a test on a specific datasource fails, it checks the last record of the test exceptions table for that test and datasource. If the execution date is contained within the to and from dates of the last record, the test is set to PASS, the recommendation is set to the explanation from the exceptions record, and the result text is set as follows:

Test passed, based on exception approved by: effective from date to date.

The API only adds records to remove an exception. A new record should be created with new dates as needed.

This GuardAPI is available in Guardium V9.5 and later.

The REST API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/test_exception
```

GuardAPI syntax

```
create_test_exception parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| assessmentDesc | String | |
| assessmentScope | String | |
| datasourceGroup | String | |
| datasourceName | String | |
| datasourceScope | String | |
| datasourceType | String | For valid values, call <code>create_test_exception</code> from the command line with <code>--help=true</code> . |
| explanation | String | Required. A recommendation as to why the test passes. |
| fromDate | String | |
| testDescription | String | Required. A valid test name within Security Assessments. |
| toDate | String | |

Examples

```
grdapi create_test_exception datasourceName=ORAPROD5 testDescription="CVE-2009-0997" fromDate="2012-07-01 08:00:00"  
toDate="2012-07-31 08:00:00" explanation="Currently in testing stage"
```

create_update_wkc_config

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/wkc
```

GuardAPI syntax

```
create_update_wkc_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------------------|------------|--|
| action | String | Valid values: <ul style="list-style-type: none">• <code>allow</code>• <code>deny</code> |
| awsRegion | String | For valid values, call <code>create_update_wkc_config</code> from the command line with <code>--help=true</code> . |
| awsSecretManager | String | For valid values, call <code>create_update_wkc_config</code> from the command line with <code>--help=true</code> . |
| awsSecretName | String | |
| cacheSize | Integer | |
| cachetTL | Integer | |
| columnAlias | String | Valid values: <ul style="list-style-type: none">• <code>COLUMN_NAME</code>• <code>NONE</code>• <code>SHORT_UDF</code> |
| cyberarkConfig | String | For valid values, call <code>create_update_wkc_config</code> from the command line with <code>--help=true</code> . |
| cyberarkObject | String | |
| enableWkc | Boolean | Valid values: <ul style="list-style-type: none">• <code>0</code> (false)• <code>1</code> (true) Default = <code>1</code> (true) |
| hashicorpConfig | String | For valid values, call <code>create_update_wkc_config</code> from the command line with <code>--help=true</code> . |
| hashicorpPath | String | |
| hashicorpRole | String | |
| logLevel | Integer | |
| persistentCache | Boolean | Valid values: <ul style="list-style-type: none">• <code>0</code> (false)• <code>1</code> (true) Default = <code>1</code> (true) |
| persistentCacheMaxEntries | Integer | |
| persistentCacheMaxFiles | Integer | |
| persistentCacheTTL | Integer | |
| units | String | |
| userScope | String | Valid values: <ul style="list-style-type: none">• <code>dbuser</code>• <code>appuser</code> |
| wkcURI | String | |
| wkcUser | String | |
| wkcUserPwd | String | |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

create_user

Add a user to your Guardium® system.

Users are created with the `user` role. Use the [set user roles](#) API to change or add other roles.

Note: Before a user can access the GuardAPIs with one of the default CLI accounts (guardcli1,...guardcli9), you must authenticate them by using the set guiluser CLI command. For more information, see [User account, password, and authentication CLI Commands](#).
This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/user
```

GuardAPI syntax

```
create_user parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------|------------|---|
| confirmPassword | String | Required. Confirm the password. The confirmPassword must match the value of Password. |
| country | String | The ISO 3166 2-letter country code for this user, such as US or ES. For valid values, call <code>create_user</code> from the command line with <code>--help=true</code> . |
| disabled | Boolean | <p>Enables or disables this user. Valid values:</p> <ul style="list-style-type: none"> • 0 (false): The user is enabled. • 1 (true): The user is disabled. <p>Default = 0 (enabled)</p> |
| disablePwdExpiry | Boolean | <p>Enables or disables the requirement that a user to reset their password the first time they log in.</p> <p>Valid values:</p> <ul style="list-style-type: none"> • 0 (false): A user must reset their password on first login. • 1 (true): The password does not expire on first login. <p>Default = 0 (false)</p> |
| email | String | |
| firstName | String | Required. |
| lastName | String | Required. |
| password | String | Required. The password must be at least 8 characters long and include at least one of each: <ul style="list-style-type: none"> • An uppercase letter (A-Z) • A lowercase letter (a-z) • A number (0-9) • A special character, which can be: at sign (@), hashtag (#), dollar sign (\$), percent sign (%), caret (^), ampersand (&), asterisk (*), exclamation (!), hyphen (-), underscore (_), plus (+), or equals (=). |
| smartCardUserName | String | Common name in the certificate.
Enter the smart card user name when smart card authentication is turned on. |
| userName | String | Required. A username for this user.
The following characters are not allowed in usernames : semicolon (;), forward slash (/), dollar sign (\$), and percent sign (%). |

Examples

For example, the following API creates a user with the username Fred McDerf:

```
grdapi create_user firstName=Fred lastName=McDerf password=Furball123!
confirmPassword=Furball123! userName="Fred McDerf" disabled=false
```

Sample output:

```
ID=20001
ok
```

Related concepts

- [User account, password, and authentication CLI Commands](#)

Related reference

- [list_roles](#)
- [set_user_roles](#)
- [update_user](#)

create_user_hierarchy

This command creates a relationship between a user and parent in the user data security hierarchy.

Note: An error occurs if the insert is circular (that is, a parent reports to a child).

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/user_hierarchy
```

GuardAPI syntax

```
create_user_hierarchy parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| parentUserName | String | Required. The name of the parent user. |
| userName | String | Required. The name of the user with a relationship to the parent user. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi create_user_hierarchy parentUserName=AdminManager userName=Admin1
```

Related concepts

- [Data Security - User Hierarchy and Database Associations](#)

datamart_copy_file_bundle

This command creates and manages data mart bundles for user-defined and predefined file data marts.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/datamart_copy_file_bundle
```

GuardAPI syntax

```
datamart_copy_file_bundle parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------------|------------|---|
| action | String | Required. Valid values: <ul style="list-style-type: none">• <i>create</i>: creates a bundle• <i>delete</i>: deletes a bundle• <i>include</i>: adds a data mart to a bundle• <i>exclude</i>: removes a data mart from a bundle• <i>info</i>: returns details on a bundle |
| bundle_name | String | Required for all actions. Name of the bundle. |
| datamart_name | String | Required when action=include or exclude. The name of the data mart. |
| main_datamart_name | String | Required when action=create. The name of the main data mart. The main data mart must have the latest scheduled extraction time of all the data marts in the bundle, so that it can include all the other data marts' latest extracts. |

Examples

This example creates a bundle named DMbundle33, with a main data mart of Export:Access Log.

```
datamart_copy_file_bundle action=create bundle_name=DMbundle33 main_datamart_name="Export:Access Log"
```

This example adds the Export:Outliers List data mart to the bundle DMbundle33.

```
datamart_copy_file_bundle action=include bundle_name= datamart_name="Export:Outliers List"
```

Related concepts

- [Data mart](#)

Related reference

- [Data mart APIs](#)

datamart_include_file_header

This command controls whether the header line (column names) are included in the output CSV of a user-defined and predefined file data mart.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/datamart_include_file_header
```

GuardAPI syntax

```
datamart_include_file_header parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------|------------|--|
| includeFileHeader | String | Required. Valid values: <ul style="list-style-type: none">• Yes• No |
| Name | String | Required. Data mart name. |

Examples

This command enables the file header on the data mart Export:Exception Log.

```
grdapi datamart_include_file_header Name=Export:Exception Log includeFileHeader=Yes
```

Related concepts

- [Data mart](#)

Related reference

- [Data mart APIs](#)

datamart_refresh_metadata

Run this command to transfer data mart metadata from the central manager to the specified managed unit.

Data mart metadata is saved on a central manager and propagated to its managed units during the user synchronization job, which runs every 30 minutes by default. If, for example, you configured the data mart to send data to the external server by running `grdapip datamart_update_copy_file_info`. Now you want to run the data mart itself on one of the managed units, to extract data and send it to the target external server. But the server information is not there yet. Run this command `grdapip datamart_refresh_metadata` to transfer this information to this specific unit, so that you can successfully run the data mart.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/datamart_refresh_metadata
```

GuardAPI syntax

```
datamart_refresh_metadata parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------|------------|--|
| unit_hostname | String | Required. Guardium hostname or IP address. |

Examples

To send data mart metadata to the managed unit with IP 9.9.9.9:

```
grdapip datamart_refresh_metadata unit_hostname=9.9.9.9
```

Related concepts

- [Data mart](#)

Related reference

- [Data mart APIs](#)

datamart_run_once_now

This command runs the specified datamart, once, starting when you run the command.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/datamart_run_once_now
```

GuardAPI syntax

```
datamart_run_once_now parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------|------------|-------------|
| datamart_name | String | Required. |

Examples

To run the data mart Export:Full SQL:

```
grdapic datamart_run_once_now datamart_name="Export:Full SQL"
```

Related concepts

- [Data mart](#)

Related reference

- [Data mart APIs](#)

datamart_set_active

This command activates extraction of the specified datamart.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/datamart_set_active
```

GuardAPI syntax

```
datamart_set_active parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------------------------|
| Name | String | Required. A defined data mart |

Examples

To activate the datamart Export:Full SQL:

```
datamart_set_active name="Export:Full SQL"
```

Related concepts

- [Data mart](#)

Related reference

- [Data mart APIs](#)

datamart_set_date_format

Use this command if the default date format of a user-defined or predefined export datamart does not meet the requirements of your target server.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/datamart_set_date_format
```

GuardAPI syntax

```
datamart_set_date_format parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|--------------------------------|
| datamart_name | String | Required. |
| new_date_format | String | Required. New date format. |
| old_date_format | String | Required. Current date format. |

Examples

To change the date format to %Y-%m-%dT%TZ:

```
grdapi datamart_set_date_format datamart_name="Export:Full SQL" old_date_format="%Y-%m-%dT%T" new_date_format="%Y-%m-%dT%TZ"
```

Related concepts

- [Data mart](#)

Related reference

- [Data mart APIs](#)

datamart_set_inactive

This command de-activates extraction of the specified data mart.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/datamart_set_inactive
```

GuardAPI syntax

```
datamart_set_inactive parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---------------------------|
| Name | String | Required. Data mart name. |

Examples

To deactivate the data mart Export:Full SQL:

```
datamart_set_inactive name="Export:Full SQL"
```

Related concepts

- [Data mart](#)

Related reference

- [Data mart APIs](#)

datamart_update_copy_file_info

This command modifies a user-defined and predefined file data mart export.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/datamart_update_copy_file_info
```

GuardAPI syntax

```
datamart_update_copy_file_info parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------------|------------|---|
| destinationHost | String | Required. Hostname of target server. |
| destinationPass word | String | Required if you are using a username and password for authentication. Password for the user specified by destinationUser. |
| destinationPath | String | Required. Path to location to store the data mart extraction. |
| destinationPort | String | Required. The port number for the destination. |
| destinationUser | String | Required. User with write access to the destination path. |
| failoverDestinationHost | string | If the export to destinationHost fails, then Guardium attempts to export the files to failoverDestinationHost. destinationHost and failoverDestinationHost must have the same credentials and path (destinationPath). The output to get_datamart_info shows the server to which results were last sent. |
| Name | String | Required. Data mart name |
| ssh_key_active | Boolean | Enables data transfer using the SSH key. Enable the SSH key feature with the CLI command store system scp-ssh-key-mode on . Generate ssh-key pairs and copy the public part of the key, public-transfer-key , to the remote host. For more information, see Enabling ssh-key pairs for data archive, data export, data mart . Valid values: <ul style="list-style-type: none">• 0: Disable• 1: Enable Default = 0 |
| transferMethod | String | Required. Valid values: <ul style="list-style-type: none">• SCP• FTP |
| validate | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| withCOMPLETEfile | Boolean | A complete file is sent after a data file is successfully transferred. Valid values: <ul style="list-style-type: none">• 0 (false): The marker file is not sent and the data file is prefixed with "DMv2_". For example: DMv2_vmappibm_EXP_SYSTEM_INFO_20170508150000.gz• 1 (true): Two files are sent, one with data and another empty file with the word COMPLETE in it. The second file is a marker that the result is complete. The format of the file name is <global prefix ID>_<appliance name>_<datamart name>_<timestamp>.gz, for example: 1234567890123456789_vmappibm_EXP_SYSTEM_INFO_20170508150000.gz2. Default = 1 (true) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Example

To update the Export:Session Log transfer method to SCP:

```
grdapi datamart_update_copy_file_info destinationHost=server22 destinationPassword=passpass destinationPath=<destination server> destinationUser=useruser Name="Export:Session Log" transferMethod=SCP
```

Related concepts

- [Data mart](#)
- [System CLI Commands](#)

Related reference

- [Data mart APIs](#)

datamart_validate_copy_file_info

This command validates the connection to the target host for user-defined or predefined file data mart export.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/datamart_validate_copy_file_info
```

GuardAPI syntax

```
datamart_validate_copy_file_info parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------------|------------|--|
| destinationHost | String | Required. Hostname of target server. |
| destinationPassword | String | Password for the user specified by destinationUser. |
| destinationPath | String | Required. Path to location to store the datamart extraction. |
| destinationUser | String | Required. User with write access to the destination path. |
| failoverDestinationHost | string | If the export to destinationHost fails, then Guardium attempts to export the files to failoverDestinationHost. destinationHost and failoverDestinationHost must have the same credentials and path (destinationPath). The output to get_datamart_info shows the server to which results were last sent. |
| ssh_key_active | Boolean | Enables data transfer using the SSH key. Enable the SSH key feature with the CLI command store system scp-ssh-key-mode on . Generate ssh-key pairs and copy the public part of the key, public-transfer-key , to the remote host. For more information, see Enabling ssh-key pairs for data archive, data export, data mart . Valid values: <ul style="list-style-type: none">• 0: Disable• 1: Enable Default = 0 |
| transferMethod | String | Valid values: <ul style="list-style-type: none">• SCP• FTP |
| transferMethod | String | Valid values: <ul style="list-style-type: none">• SCP• FTP |

Examples

```
grdapi datamart_validate_copy_file_info destinationHost=hostname destinationUser=user22 destinationPassword= destinationPath= Name= transferMethod=
```

Related concepts

- [Data mart](#)

Related reference

- [Data mart APIs](#)

delete_adhoc_policy_analyzer

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/delete_adhoc_policy_analyzer
```

GuardAPI syntax

```
delete_adhoc_policy_analyzer parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| scheduleId | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

delete_alerter_snmp_settings

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/delete_alerter_snmp
```

GuardAPI syntax

```
delete_alerter_snmp_settings parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

delete_alias

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/alias
```

GuardAPI syntax

```
delete_alias parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------|------------|---|
| dbValue | String | Required. |
| groupTypeDesc | String | Required. For valid values, call delete_alias from the command line with <code>--help=true</code> . |

delete_allowed_db_by_entry_id

This command removes a User-DB association by the user's ID.

You can find the ID by using the [list_allowed_db_by_user](#) API.

Note: To apply the changes to the active User-DB association map, run [update_user_db](#) after you run this command.
This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/allowed_db
```

GuardAPI syntax

```
delete_allowed_db_by_entry_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| id | Long | Required. The record ID of the User-DB association. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapic delete_allowed_db_by_entry_id id=2
```

Sample output

```
ID=0
Number of matches: 1
When complete, in order for synchronization to take effect, run update_user_db
ok
```

Related reference

- [list_allowed_db_by_user](#)
- [update_user_db](#)

delete_allowed_db_by_user

This command removes a User-DB association by the user's name.

Note: To apply the changes to the active User-DB association map, run [update_user_db](#) after you run this command.
This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/allowed_db
```

GuardAPI syntax

```
delete_allowed_db_by_user parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------|------------|---|
| instanceName | String | A specific instance name within the server. |
| serverIp | String | The server IP. |
| userName | String | Required. The name of the user. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi delete_allowed_db_by_user userName=Fred
```

Sample output

```
ID=2
When complete, in order for synchronization to take effect, run update_user_db
ok
```

Related concepts

- [Data Security - User Hierarchy and Database Associations](#)

Related reference

- [update_user_db](#)

delete_analytic_user_feedback

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/delete_analytic_user_feedback
```

GuardAPI syntax

```
delete_analytic_user_feedback parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|-------------|
| feedback_id | Long | |

delete_api_parameter_mapping

Add a short description here.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `DELETE` method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/param_mapping_for_function
```

GuardAPI syntax

```
delete_api_parameter_mapping parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| attributeLabel | String | Required. |
| domain | String | Required. |
| entityLabel | String | Required. |
| functionName | String | Required. |
| parameterName | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

delete_approved_stap_client

This command removes an approved database from the list of databases allowed to communicate with the S-TAP®. As a result, its S-TAPs are no longer allowed to access and communicate with the Guardium® system.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/approved_stap_client
```

GuardAPI syntax

```
delete_approved_stap_client parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| stapHost | String | Required. The host name or IP address of the database server on which the S-TAP is installed. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To delete the database server with the IP of 12.12.12.12 from the list of databases that are allowed to communicate with the Guardium system:

```
grdapi delete_approved_stap_client stapHost=12.12.12.12
```

Related tasks

- [Allow \(approve\) S-TAP connection to Guardium \(S-TAP Certification\)](#)

Related reference

- [S-TAP and inspection engine APIs](#)

delete_archive_configuration

This command deletes the scheduled data archive on one or more Guardium® systems.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/delete_archive_configuration
```

GuardAPI syntax

```
delete_archive_configuration parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To delete the configured archive on the system on which you enter the command:

```
grdapi delete_archive_configuration
```

Related tasks

- [Managing stored data](#)

Related reference

- [Archive, export, import, purge, and restore APIs](#)

delete_assessment

This command to deletes a security assessment.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/assessment
```

GuardAPI syntax

```
delete_assessment parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|--|
| assessmentDescription | String | Required. |
| forceDelete | Boolean | <p>Valid values:</p> <ul style="list-style-type: none">• 0 (false)• 1 (true) <p>Default = 0 (false)</p> |

Example

```
grdapi delete_assessment assessmentDescription=Assess1
```

delete_assessment_datasource

This command deletes a datasource from a security assessment.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/assessment_datasource
```

GuardAPI syntax

```
delete_assessment_datasource parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|--|
| assessmentDescription | String | Required. This string is a variable that is unique. Ensure that there is no previous assessment with the same description. If a previous assessment exists, an error occurs. |
| datasourceName | String | Required. This string is a variable, and must be the name of an existing data source. If a datasource with the defined string is not present, then an error occurs. |

Example

```
grdapi delete_assessment_datasource assessmentDescription=Assess1 datasourceName=DS1
```

delete_assessment_datasource_group

This command deletes an assessment from a datasource group.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/assessment_datasource_group
```

GuardAPI syntax

```
delete_assessment_datasource_group parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|-------------|
| assessmentDescription | String | Required. |
| groupName | String | Required. |

delete_assessment_test

This command deletes a test from an existing security assessment.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/assessment_test
```

GuardAPI syntax

```
delete_assessment_test parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|---|
| assessmentDescription | String | Required. |
| datasourceType | String | For valid values, call delete_assessment_test from the command line with --help=true. |
| testDescription | String | Required. |

Example

```
grdapi delete_assessment_test assessmentDescription=Assess1
```

delete_audit_process

Deletes an audit process.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/audit_process
```

GuardAPI syntax

```
delete_audit_process parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| force | Boolean | Delete the audit process even if contains results. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| processName | String | Required. Use list_audit_processes to find the name of the audit process to delete. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Related concepts

- [Building audit processes](#)

delete_audit_process_result

This command deletes certain specified audit process results.

To run this command you must have the audit-delete role.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/audit_process_result
```

GuardAPI syntax

```
delete_audit_process_result parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------|------------|--|
| ExecutionDateFrom | String | Required. Audit process start time. |
| ExecutionDateTo | String | Required. Audit process end time. |
| ProcessName | String | Required. Audit process name. For valid values, call delete_audit_process_result from the command line with --help=true. |

Related concepts

- [Building audit processes](#)
- [Understanding roles](#)

Related reference

- [execute_auditProcess](#)
- [list_audit_processes](#)

delete_autodetect_process

Use this command to delete an auto-discovery process and all of its associated tasks. You cannot run this command on a process that is running or is scheduled.

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the `DELETE` method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/autodetect_processes
```

GuardAPI syntax

```
delete_autodetect_process parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| process_name | String | Required. Name of the auto-discovery process |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To delete the auto-discovery process myProcess:

```
grdapi delete_autodetect_process process_name=myProcess
```

Related concepts

- [Database auto-discovery](#)

Related reference

- [Auto-discovery APIs](#)

delete_autodetect_scans_for_process

Use this command remove all the tasks for a process on the specified hostnames and ports. You cannot run this command on a process that is running or scheduled, or has results.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/autodetect_scans_for_process
```

GuardAPI syntax

```
delete_autodetect_scans_for_process parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| hostList | String | Lists of hosts. Space separated list of IPs or IP ranges and wild cards such as 192.168.0.1 192.168.1.* |
| portList | String | List of ports. Comma separated list of ports or port ranges such as 22,23,1400-1600. |
| process_name | String | Required. Name of the auto-discovery process |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To delete the auto-discovery process myProcess from the hosts 192.168.1.1 and 192.168.1.3, on ports 22 and 23:

```
grdapi delete_autodetect_scans_for_process hostList="192.168.1.1 192.168.1.3" portList="22,23"
```

Related concepts

- [Database auto-discovery](#)

Related reference

- [Auto-discovery APIs](#)

delete_available_test_notes

This API is available in Guardium v11.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/available_test_notes
```

GuardAPI syntax

```
delete_available_test_notes parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|---|
| datasourceType | String | Required. For valid values, call <code>delete_available_test_notes</code> from the command line with <code>--help=true</code> . |

| Parameter | Value type | Description |
|-----------------|------------|-------------|
| testDescription | String | Required. |

delete_aws_secrets_manager_config

Use this command to delete an AWS secrets configuration.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/aws_secrets_manager
```

GuardAPI syntax

```
delete_aws_secrets_manager_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| name | String | Required. |

Examples

```
grdapapi delete_aws_secrets_manager_config name="GRDAPI IAM-Instance-Profile"
grdapapi delete_aws_secrets_manager_config name="GRDAPI IAM-Role"
grdapapi delete_aws_secrets_manager_config name="GRDAPI Security-Credentials"
```

delete_cas_host

This command removes a Configuration Auditing System (CAS) host configuration. A CAS host configuration defines one or more CAS host instances, and each CAS host instance specifies a CAS template set.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/cas_host
```

GuardAPI syntax

```
delete_cas_host parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| hostName | String | Required. The name or IP address of the host configuration to delete. |
| osType | String | Required. The operating system of this host. The OS type can be either: <ul style="list-style-type: none"> • UNIX • WIN |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

delete_cas_host_instance

This command removes a Configuration Auditing System (CAS) host instance. A CAS host configuration defines one or more CAS host instances, and each CAS host instance specifies a CAS template set.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/cas_host_instance
```

GuardAPI syntax

```
delete_cas_host_instance parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|---|
| datasourceName | String | Required. The data source of the host instance to delete. |
| templateSetLabel | String | Required. The name of the template set associated with this host instance. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

delete_cas_template

This command removes a Configuration Auditing System (CAS) template from a template set.

Note: You cannot delete a predefined template.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/cas_template
```

GuardAPI syntax

```
delete_cas_template parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|--|
| templateId | Long | Required. The ID of the template you want to delete. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To delete a CAS template from a template set:

```
curl -k --header "Authorization: Bearer 8ad14246-8815-4043-ab19-074d6bfcaad3" -i -X
DELETE -d '{"templateId":"20003"}'
https://localhost:8443/restAPI/cas_template
```

Related concepts

- [Configuration Auditing System \(CAS\)](#)

Related reference

- [Configuration Auditing System \(CAS\) APIs](#)

delete_cas_template_set

This command removes a Configuration Auditing System (CAS) template set from a CAS host instance.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `DELETE` method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/cas_template_set
```

GuardAPI syntax

```
delete_cas_template_set parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|---|
| templateSetLabel | String | Required. The name of the template set to remove. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

delete_classifier_action

The command deletes classification actions.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/classifier_action
```

GuardAPI syntax

```
delete_classifier_action parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|-------------|
| actionName | String | Required. |
| policyName | String | Required. |
| ruleName | String | Required. |

Examples

```
grdapi delete_classifier_action policyName=access_policy ruleName=access_rule actionName=log_access
```

delete_classifier_document_rule

This API is available in Guardium V11.4 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/classifier_document_rule
```

GuardAPI syntax

```
delete_classifier_document_rule parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| allowlist | String | |
| enable | Boolean | Required. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| type | String | Required. Valid values: <ul style="list-style-type: none">• ALL• SSH• GUI |

delete_classifier_policy

This command deletes classification policies.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/classifier_policy
```

GuardAPI syntax

```
delete_classifier_policy parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|-------------|
| policyName | String | Required. |

Examples

```
grdapi delete_classifier_policy policyName=access_policy
```

delete_classifier_process

This command deletes classification processes.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/classifier_process
```

GuardAPI syntax

```
delete_classifier_process parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|-------------|
| processName | String | Required. |

Examples

```
grdapi delete_classifier_process processName=APITEST_Clps_10001_1
```

delete_classifier_rule

This command deletes classification rules.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/classifier_rule
```

GuardAPI syntax

```
delete_classifier_rule parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|-------------|
| policyName | String | Required. |
| ruleName | String | Required. |

Examples

```
grdapi delete_classifier_rule policyName=access_policy ruleName=access_rule
```

delete_cluster

This API deletes a specified S-TAP cluster.

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/delete_cluster
```

GuardAPI syntax

```
delete_cluster parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|-------------|
| clusterName | String | Required. |

delete_computed_attribute

This API deletes a computed attribute.

To help prevent an SQL injection attack, the following words and characters are not allowed in computed attributes:

ALTER, CREATE, DELETE, DROP, INSERT, TRUNCATE, UPDATE, semicolon (;), double-dash (--), or slash-asterisk /*)

For more information, see [create_computed_attribute](#).

This API is available in Guardium V9.5 and later.

The REST API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/computed_attribute
```

GuardAPI syntax

```
delete_computed_attribute parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| attributeLabel | String | Required. The name of the computed attribute to delete. |
| entityLabel | String | Required. The name of the main entity with which the attribute is associated, |
| expression | String | Required. The SQL expression to delete. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>; execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To delete the app_user computed attribute:

```
grdapicreate_computed_attribute  
attributeLabel="app_user" entityLabel="Access Period"  
expression="SUBSTRING_INDEX(APP_USER_NAME,char(59),1)
```

Related reference

- [create_computed_attribute](#)

delete_constant_attribute

This API is available in Guardium V9.5 and later.

The REST API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/constant_attribute
```

GuardAPI syntax

```
delete_constant_attribute parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| attributeLabel | String | Required. |
| constant | String | Required. |
| entityLabel | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

delete_cust_table_distribution_schedule

This API deletes a previously created distribution schedule for custom tables.

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/custTblDist
```

GuardAPI syntax

```
delete_cust_table_distribution_schedule parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related tasks

- [Distribute custom tables](#)

Related reference

- [sched_cust_table_distribution](#)
-

delete_custom_table_ldap_import

This command deletes a custom table that was created to import data from LDAP.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/custom_data_ldap
```

GuardAPI syntax

```
delete_custom_table_ldap_import parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| importId | Integer | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

delete_cyberark_config

This command deletes a CyberArk configuration from your Guardium system.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/cyberark
```

GuardAPI syntax

```
delete_cyberark_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| name | String | Required. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

delete_datasourceRef_by_id

This command removes a datasource reference for a specific object of a specific application type. The datasource, object, and application type are referenced by identification keys.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/datasource_ref
```

GuardAPI syntax

```
delete_datasourceRef_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| appId | Integer | <p>Required. Identifies the application type.
Valid values:</p> <ul style="list-style-type: none"> • 8 (security assessment) • 47 (custom tables) • 51 (classifier) |
| datasourceId | Integer | Required. Identifies the datasource by its identification key. |
| objId | Integer | Required. Identifies an instance of the specified appId type. For example, if <code>appId=51</code> , objId is the identification key of a classification process. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapic delete_datasourceRef_by_id appId=51 datasourceId=2 objId=1
```

delete_datasourceRef_by_name

This command removes a datasource reference for a specific object of a specific application type. The datasource, object, and application type are referenced by name.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/datasource_ref
```

GuardAPI syntax

```
delete_datasourceRef_by_name parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| application | String | Required. Identifies the application type. For valid values, call delete_datasourceRef_by_name from the command line with --help=true. |
| datasourceName | String | Required. Identifies the datasource by its name. For valid values, call delete_datasourceRef_by_name from the command line with --help=true. |
| objName | String | Required. For valid values, call delete_datasourceRef_by_name from the command line with --help=true. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

delete_datasource_by_id

This command deletes a datasource definition identified by an identification key.

This command deletes the specified datasource definition regardless of who created it.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/delete_datasource_by_id
```

GuardAPI syntax

```
delete_datasource_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------------|------------|---|
| cascade | Boolean | <p>Lists all the applications where the datasource is referenced. It also displays a confirmation number. Valid values:</p> <ul style="list-style-type: none">• 0 (false)• 1 (true) <p>Default = 0 (false)</p> |
| confirmationNumber | Integer | When the confirmation number is used, all references of the datasource are deleted. Default = 0 |
| id | Integer | Required. The identification key of the datasource to be deleted. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Use this command to delete a datasource with identification key 2:

```
grdapi delete_datasource_by_id id=2
```

delete_datasource_by_name

This command deletes a datasource definition identified by name.

This command deletes the specified datasource definition regardless of who created it.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/datasource
```

GuardAPI syntax

```
delete_datasource_by_name parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------------|------------|---|
| cascade | Boolean | <p>Lists all the applications where the datasource is referenced. It also displays a confirmation number. Valid values:</p> <ul style="list-style-type: none">• 0 (false)• 1 (true) <p>Default = 0 (false)</p> |
| confirmationNumber | Integer | When the confirmation number is used, all references of the datasource are deleted. Default = 0 |
| name | String | Required. The datasource name. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Use this command to delete a datasource with the name swanSybase:

```
grdapi delete_datasource_by_name name=swanSybase
```

delete_datasource_configuration

This API is available in Guardium v12.0 and later.

GuardAPI syntax

```
delete_datasource_configuration parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|-------------|
| ucDatasourceId | Integer | Required. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

delete_datasource_custom_property

This command deletes a custom property that was configured for your datasource.

This API is available in Guardium V11.4 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/datasource_custom_prop
```

GuardAPI syntax

```
delete_datasource_custom_property parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| force | Boolean | <p>When <code>force="1"</code> the custom property is deleted even if it's being used by a datasource.</p> <p>Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true) |
| name | String | Required. The name of the property to delete. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Example

The following command deletes the custom property "Business Unit" and removes it from all the datasources and datasources groups to which the property is assigned.

```
grdapl delete_datasource_custom_property name="Business Unit" force="1"
```

Related concepts

- [Datasource APIs](#)

delete_datasource_group

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/datasource_group
```

GuardAPI syntax

```
delete_datasource_group parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| groupName | String | Required. |

delete_datasource_groupRef_by_id

Delete datasource groups that are in security assessments, discovery scenarios, or custom tables.

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/datasource_group_ref
```

GuardAPI syntax

```
delete_datasource_groupRef_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------|------------|---|
| appId | Integer | Required. For valid values, call delete_datasource_groupRef_by_id from the command line with --help=true. |
| datasourceId | Integer | Required. The ID of the datasource. |
| objId | Integer | Required. The object ID of the security assessment, discovery scenario, or custom table. |

delete_datasource_groupRef_by_name

Delete datasource groups that are in security assessments, discovery scenarios, or custom tables.

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/datasource_group_ref
```

GuardAPI syntax

```
delete_datasource_groupRef_by_name parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------------|------------|---|
| application | String | Required. For valid values, call delete_datasource_groupRef_by_name from the command line with --help=true. |
| datasourceGroupName | String | Required. The name of the datasource group. |
| objName | String | Required. The name of the security assessment, discovery scenario, or custom table. |

delete_db_user_mapping

This command deletes the mappings between DB user and email address for real-time alerts.

You can use a percent (%) wildcard for all parameters.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/db_user_mapping
```

GuardAPI syntax

```
delete_db_user_mapping parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| dbUserName | String | Required. The DB username. |
| emailAddress | String | Required. For real-time alerts, the email address that maps to the DB user. The at symbol (@) is required. |
| serverIp | String | Required. The server IP address. You can use % wildcards for any element in the IP address. For example: <ul style="list-style-type: none">• 192.168.2.%• 2620:1f7:807%:920:% |
| serviceName | String | Required. The server name. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GuardAPI example

```
grdapi delete_db_user_mapping serverIp=192.168.%.% serviceName=ora1 dbUserName=hadrian emailAddress=hadrian.swall@%..com
```

Related concepts

- [Alerting rule actions](#)

Related reference

- [create_db_user_mapping](#)

delete_distributed_report_result_for_period

Run this API to delete a distributed report result for the specified period.

For example, a distributed report has a one day time granularity, it collects data from aggregators, and is scheduled to run daily at 1am. One of the aggregators had not received data from all of its collectors before its previous run. To get a complete report, you need to delete the results of this incomplete run, and rerun the distributed report manually (with the API [rerun_distributed_report](#)) for this period.

This API is available in Guardium V10.1.4 and later.

GuardAPI syntax

```
delete_distributed_report_result_for_period parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| endTime | Date | Required. |
| hostname | String | Required. |
| reportId | Integer | Required. |

| Parameter | Value type | Description |
|------------|------------|--|
| runOptions | String | Required. Valid values: <ul style="list-style-type: none"> • <i>fromHostname</i> • <i>fromAllUnits</i> |
| startTime | Date | Required. |

Related concepts

- [Distributed report builder](#)

Related reference

- [Reports and report generation APIs](#)

delete_ef_mapping

This function deletes an external feed mapping.

To protect predefined Guardium mappings, only mappings with an identification key greater than 20000 can be deleted.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/delete_ef_mapping
```

GuardAPI syntax

```
delete_ef_mapping parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| reportName | String | Required. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> • <i>all_managed</i>: execute on all managed units but not the central manager • <i>all</i>: execute on all managed units and the central manager • <i>group:<group name></i>: execute on all managed units identified by <i><group name></i> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <i>api_target_host=10.0.1.123</i>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <i>api_target_host=10.0.1.123</i>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

Use this command to delete the *Sessions per Day* mapping:

```
grdapic delete_ef_mapping reportName="Sessions per Day"
```

delete_entry_location

This command removes the specified catalog entry if you specify a file name. If you do not specify a file name, this command removes the catalog entries for the specified path and hostname.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/entry_location
```

GuardAPI syntax

```
delete_entry_location parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| fileName | String | Identifies a single catalog entry to remove. If omitted, all catalog entries on the specified hostname and path are deleted. |
| hostName | String | Required. The hostname or IP address. |
| path | String | Required. The path to the archive directory. <ul style="list-style-type: none">• Amazon S3: bucket name• IBM COS: bucket name• EMC Centera: Centera clipID• FTP: Specify the directory relative to the FTP account home directory.• SCP: Specify the directory as an absolute path.• IBM Cloud: Container• TSM: path |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GuardAPI example

```
grdapi delete_entry_location path=/var/dump/henry hostName=192.168.1.18
```

Related tasks

- [Data and result catalogs](#)

Related reference

- [Archive, export, import, purge, and restore APIs](#)
- [Catalog entry APIs](#)

delete_export_configuration

Use this command to delete a defined data export configuration on one or more Guardium® systems.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/delete_export_configuration
```

GuardAPI syntax

```
delete_export_configuration parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To delete the configured data export on the system on which you enter the command:

```
grdapi delete_export_configuration
```

Related tasks

- [Managing stored data](#)

Related reference

- [Archive, export, import, purge, and restore APIs](#)

delete_group_by_desc

This command deletes a group identified by its description.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/group
```

GuardAPI syntax

```
delete_group_by_desc parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| desc | String | Required. Identifies the group by its description. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Use this command to delete a group with the description *A group*:

```
grdapi delete_group_by_desc desc="A group"
```

delete_group_by_id

This command deletes a group identified by its identification key.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/group
```

GuardAPI syntax

```
delete_group_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| id | Integer | Required. Identifies the group by its identification key. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Use this command to delete a group with the identification key 100003:

```
grdapic delete_group_by_id id=100003
```

delete_group_from_quick_search

This command deletes a group from the quick search facet drop-down menus. After you delete it, you will not be able to select it to filter the investigation dashboard results.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
delete_group_from_quick_search parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|--|
| facet | String | Required. The facet of the group you are deleting. Valid values: <ul style="list-style-type: none">• DB_USER• OS_USER• OBJECT• VERB• FAM_COMMAND• SERVER_IP |
| group_descripti
on | String | Required. Group name you are deleting, of the specified facet type. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To delete server_group5 to the quick search:

```
delete_group_from_quick_search facet=SERVER_IP group_description=server_group5
```

Related concepts

- [Investigation dashboard](#)

Related reference

- [Investigation dashboard APIs](#)

delete_hashicorp_config

Use this command to delete a HashiCorp configuration from your Guardium® system.

This API is available in Guardium v11.4 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/hashicorp
```

GuardAPI syntax

```
delete_hashicorp_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| name | String | Required. For valid values, call <code>delete_hashicorp_config</code> from the command line with <code>--help=true</code> . |

Example

```
grdapic delete_hashicorp_config name="No SSL User and password API"
```

delete_hierarchical_member_from_group_by_desc

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/hierarchical_member
```

GuardAPI syntax

```
delete_hierarchical_member_from_group_by_desc parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| desc | String | Required. |
| member | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

delete_imscheckpoint_record

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `DELETE` method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/ims_checkpoint
```

GuardAPI syntax

```
delete_imscheckpoint_record parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------|------------|-------------|
| agentName | String | Required. |
| context | String | Required. |
| imsName | String | Required. |
| logStreamName | String | Required. |

delete_inactive_stap

Use this command to delete an inactive S-TAP® (or all S-TAPs) on the specified S-TAP host, or all hosts, on one or all collectors that send data to the specified S-TAP host.

To identify inactive S-TAPs, use the API command `list_staps` or view the report Inactive S-TAPs Since.

Table 1. `stapHost` and `api_target_host` values and the resulting affected S-TAPs

| stapHost | api_target_host | Command affects: |
|---------------------|----------------------------------|------------------------------|
| specific S-TAP host | specific target host / collector | S-TAP on the collector |
| all | specific target host / collector | All S-TAPs on the collector |
| specific S-TAP host | all_managed | S-TAP on all collectors |
| all | all_managed | All S-TAPs on all collectors |

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/delete_inactive_stap
```

GuardAPI syntax

```
delete_inactive_stap parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| force | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| stapHost | String | Valid values: <ul style="list-style-type: none">• specific S-TAP host• all |
| api_target_host | String | Specifies where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• group:<group name>: execute on all managed units identified by <group name>• Host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123. |

Examples

To delete inactive S-TAPs that are configured to send data to the Guardium system on which you enter the command:

```
grdapi delete_inactive_stap
```

Related reference

- [S-TAP and inspection engine APIs](#)

delete_invalid_stap

Use this command to remove invalid S-TAPs from the Deployment Health Topology view, for example. This command deletes invalid S-TAPs, and not inactive S-TAPs.

This API is available in Guardium V10.6 and later.

GuardAPI syntax

```
delete_invalid_stap parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To delete invalid S-TAPs from a collector:

```
grdapi delete_invalid_stap debug=3
```

To delete invalid S-TAPs from the collector XXXX, enter this command on the collector's central manager:

```
grdapi delete_invalid_stap api_target_host=XXXX debug=3
```

To delete all invalid S-TAPs from in a centralized system, enter this command on the central manager:

```
grdapi delete_invalid_stap api_target_host=all debug=3
```

Related concepts

- [Deployment health topology and table views](#)
- [S-TAP and GIM dashboard](#)

[delete_kafka_cluster](#)

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/kafka_cluster
```

GuardAPI syntax

```
delete_kafka_cluster parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|-------------|
| clusterName | String | |

[delete_member_from_group_by_desc](#)

Remove a member from a group identified by its description.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/group_member
```

GuardAPI syntax

```
delete_member_from_group_by_desc parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| desc | String | Required. Identifies the group by its description. |
| member | String | Required. Identifies the name of the group member to be removed. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

Use this command to remove the member *boston* from the group *A group*:

```
grdapic delete_member_from_group_by_desc desc="A group" member=boston
```

[delete_member_from_group_by_id](#)

Remove a member from a group identified by its identification key.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/group_member_by_group_id
```

GuardAPI syntax

```
delete_member_from_group_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| id | Integer | Required. Identifies the group by its identification key. |
| member | String | Required. Identifies the name of the group member to be removed. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group: <group name>; execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Use this command to remove the member `turkey` from the group with identification key `100005`:

```
grdapi delete_member_to_group_by_id id=100005 member=turkey
```

delete_oauth_clients

This API removes the API clients that were registered with the `register_oauth_client` API.

This API is available in Guardium V11.2 and later.

GuardAPI syntax

```
delete_oauth_clients parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| client_id | String | The ID of a specific client to delete. |
| all | String | Delete all API clients. |

Examples

```
grdapi delete_oauth_clients client_id=123
```

```
grdapi delete_oauth_clients all
```

Related reference

- [register_oauth_client](#)

delete_policy

This command deletes an existing policy.

[policy_uninstall](#) API uninstalls a policy, but does not delete it.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/policy
```

GuardAPI syntax

```
delete_policy parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| policyDesc | String | Required. The name of the policy to delete. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi delete_policy policyDesc="My Hadoop Policy"
```

Related reference

- [policy_uninstall](#)

delete_quarantine

This command deletes an existing quarantine for a specified user.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `DELETE` method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/quarantine
```

GuardAPI syntax

```
delete_quarantine parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|--|
| dbUser | String | Required. The name of the quarantined database user. |
| serverIp | String | Required. The server IP address. |
| serviceName | String | Required. The server name. |
| type | String | Required. If the database is not IBM Z® or IMS, specify <code>normal</code> . Valid values: <ul style="list-style-type: none">• <code>normal</code>• <code>DB2Z</code>• <code>IMS</code> |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

The following command ends the quarantine for this user.

```
grdapi delete_quarantine dbUser="Hadrian.Swall" serverIp="9.32.0.255" serviceName="company.ibm.com" type="normal"
```

Related concepts

- [Dates and Timestamps](#)
- [Logging or ignoring rule actions](#)

Related reference

- [create_quarantine_allowed_until](#)
- [create_quarantine_until](#)

delete_ranger_hdfs_config

Use this command to delete a Hadoop integration with Ranger HDFS that connects using the specified S-TAP.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/delete_ranger_hdfs_config
```

GuardAPI syntax

```
delete_ranger_hdfs_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| stapHostName | String | Required. Host name or IP of the S-TAP® that receives the Ranger audit messages from the Ranger. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related concepts

- [Hadoop integration using Ranger HDFS for Hortonworks and Cloudera 7](#)

Related reference

- [Hadoop monitoring APIs](#)
- [S-TAP Hadoop parameters](#)

delete_results_archive_configuration

Use this command to delete the configured archive of results on one or more Guardium® systems.

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/results_archive_configuration
```

GuardAPI syntax

```
delete_results_archive_configuration parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To delete the configured results archive on the system on which you enter the command:

```
grdapic delete_results_archive_configuration
```

Related tasks

- [Managing stored data](#)

Related reference

- [Archive, export, import, purge, and restore APIs](#)

delete_results_export_configuration

Use this command to delete the configured export of results on one or more Guardium® systems.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/configure_results_export
```

GuardAPI syntax

```
delete_results_export_configuration parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To delete the configured results export on the system on which you enter the command:

```
grdapi delete_results_export_configuration
```

Related tasks

- [Exporting \(files\) results](#)

Related reference

- [Archive, export, import, purge, and restore APIs](#)

delete_rule

This command removes a rule from a specified policy.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/rule
```

GuardAPI syntax

```
delete_rule parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| fromPolicy | String | Required. The name of the policy. |
| ruleDesc | String | Required. The name of the rule to remove. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi delete_rule ruleDesc="My test exception" fromPolicy="policy1"
```

delete_schedule

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/schedule
```

GuardAPI syntax

```
delete_schedule parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| deleteJob | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| jobGroup | String | Required. |
| jobName | String | Required. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

delete_sql_configuration

This command deletes the connection details between an S-TAP® and an Oracle server that is used for Oracle Unified Auditing.

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/delete_sql_configuration
```

GuardAPI syntax

```
delete_sql_configuration parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| sequence | String | Required. The sequence number of the SQL configuration to be removed within the set of SQL configurations. Use the API <code>display_stap_config</code> to list the configuration with the SQL sequence numbers. Output appears similar to with SQL_X, where X is the sequence. |
| stapHost | String | Required. The hostname of the S-TAP that connects to this Oracle DB instance. For valid values, call <code>delete_sql_configuration</code> from the command line with <code>--help=true</code> . |
| waitForResponse | String | Specifies whether the API waits for a response from the S-TAP. Valid values: <ul style="list-style-type: none">• 0 (do not wait): API exits upon updating the DB.• 1 (wait for a response): API exits after receiving a successful acknowledgement from the STAP. Default = 1 |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

delete_stap_inspection_engine

This command deletes one or more inspection engines on the specified S-TAP® host.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/inspection_engine
```

GuardAPI syntax

```
delete_stap_inspection_engine parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| sequence | Integer | The sequence number of the inspection engine to be removed within the set of inspection engines of the specified type. Use the <code>grdapi list_inspection_engines</code> command with the type option first to verify the sequence number. |
| stapHost | String | Required. The S-TAP host of the inspection engine. |
| type | String | Required. The type of data repository that is monitored.
Unix: ASTERDB, Cassandra, CockroachDB, CouchDB, DB2®, Db2 Exit, ElasticSearch, exclude IE, FTP, GreenplumDB, HADOOP, HIVE, HP-Vertica, HTTP, HUE, IMPALA, Informix®, Informix Exit, KERBEROS, MariaDB, MemSQL, MongoDB, Mysql, Netezza®, Oracle, PostgreSQL, REDIS, SAP Hana, Sybase, Teradata, Teradata Exit, WebHDFS, Windows File Share
Windows: ASTER, Cassandra, CouchDB, Db2, Db2 Exit, exclude IE, FTP, GreenplumDB, HIVE, HTTP, HUE, IMPALA, Informix, Informix Exit, MariaDB, MongoDB, MSSQL, Mysql, Oracle, PostgreSQL, Sybase, Teradata, WebHDFS, Windows File Share. |
| waitForResponse | String | <p>Specifies whether the API waits for a response from the S-TAP. Valid values:</p> <ul style="list-style-type: none"> • 0: do not wait • 1: wait for a response <p>Default = 1 when stapHost is a single host name or IP address; and 0 in all other cases.</p> |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To delete an inspection engine with sequence number = 3, from the MYSQL database with IP 11.45.12.12:

```
grdapi delete_stap_inspection_engine stapHost=11.45.12.12 sequence=3 type=mysql
```

Related concepts

- [Inspection engine configuration](#)

Related tasks

- [Linux-UNIX: Configuring an inspection engine](#)
- [Windows: Configuring an inspection engine](#)

Related reference

- [S-TAP and inspection engine APIs](#)

delete_stream

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/datasream
```

GuardAPI syntax

```
delete_stream parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| cloudTitle | String | Required. The name of the cloud DB service account. For valid values, call delete_stream from the command line with --help=true.
For more information, see Define, modify, and delete AWS cloud DB service accounts . |
| namespace | String | For Azure only. The Azure event hub namespace. |
| region | String | Required only for AWS streams. For valid values, call delete_stream from the command line with --help=true. |
| streamName | String | Required. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

delete_system_backup_configuration

This API is available in Guardium v11.4 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/configure_system_backup
```

GuardAPI syntax

```
delete_system_backup_configuration parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

delete_test_detail_exception

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `DELETE` method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/test_detail_exception
```

GuardAPI syntax

```
delete_test_detail_exception parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------------|------------|---|
| allowMultiDelete | Boolean | Required. Valid values: <ul style="list-style-type: none"> • 0 (false) • 1 (true) Default = 0 (false) |
| approver | String | |
| assessmentDesc | String | |
| assessmentScope | String | |
| datasourceGroup | String | |
| datasourceName | String | |
| datasourceScope | String | |
| datasourceType | String | |
| detailExceptionValue | String | |
| exceptionType | String | Valid values: <ul style="list-style-type: none"> • text • regex • 0 • 1 |
| fromDate | String | |
| testDescription | String | |
| toDate | String | |

delete_test_detail_exception_by_id

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `DELETE` method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/test_detail_exception
```

GuardAPI syntax

```
delete_test_detail_exception_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------|------------|-------------|
| detailExceptionId | String | Required. |

delete_test_exception

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/test_exception
```

GuardAPI syntax

```
delete_test_exception parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|--|
| allowMultiDelete | Boolean | Required. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| approver | String | |
| assessmentDesc | String | |
| assessmentScope | String | Valid values: <ul style="list-style-type: none">• CURRENT• ALL• 0• 1 |
| datasourceGroup | String | |
| datasourceName | String | |
| datasourceScope | String | Valid values: <ul style="list-style-type: none">• SINGLE• GROUP• ALL• 0• 1• 2 |
| datasourceType | String | For valid values, call delete_stream from the command line with --help=true. |
| explanation | String | |
| fromDate | String | |
| testDescription | String | |
| toDate | String | |

delete_test_exception_by_id

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/test_exception_by_id
```

GuardAPI syntax

```
delete_test_exception_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|-------------|
| testExceptionId | Long | Required. |

delete_user

This API removes a specified user from the Guardium system.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/user
```

GuardAPI syntax

```
delete_user parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| userName | String | Required. The name of the user to delete. |

Example

For example, remove Fred McDerf from your Guardium system:

```
grdapi delete_user userName="Fred McDerf"
```

Related reference

- [create_user](#)
- [list_users](#)

delete_user_hierarchy_by_entry_id

This command removes a user from a hierarchy by their ID.

You can find the ID of the user to delete with the [list_user_hierarchy_by_parent_user](#) command.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/user_hierarchy
```

GuardAPI syntax

```
delete_user_hierarchy_by_entry_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| id | Long | Required. The ID of the child user. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi delete_user_hierarchy_by_entry_id id=3
```

Related concepts

- [Data Security - User Hierarchy and Database Associations](#)

Related reference

- [create_user_hierarchy](#)
- [list_user_hierarchy_by_parent_user](#)

delete_user_hierarchy_by_user

This command removes a user from a hierarchy by their name.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/user_hierarchy
```

GuardAPI syntax

```
delete_user_hierarchy_by_user parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| userName | String | Required. The name of the user to delete from the hierarchy. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi delete_user_hierarchy_by_user userName=George
```

Related concepts

- [Data Security - User Hierarchy and Database Associations](#)

Related reference

- [create_user_hierarchy](#)

disable_advanced_threat_scanning

This command disables threat detection analytics on the specified targets.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/disable_advanced_threat_scanning
```

GuardAPI syntax

```
disable_advanced_threat_scanning parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| all | Boolean | In a central management configuration only, disables all threat detection scanners on all managed units. This is equivalent to the "all" option for the parameter api_target_host . Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To disable threat detection analytics on all managed units:

```
grdapi disable_advanced_threat_scanning all=1
```

Related concepts

- [Threat Detection Analytics](#)

Related reference

- [Threat detection analytics APIs](#)

disable_auto_execute_suggested_dependencies

This command disables job dependencies for the specified task.

This command is equivalent to deselecting the option Auto run dependent jobs in the Scheduler of a task: Guardium does not find and run all dependent jobs before running this specific jpb.

This API is available in Guardium V10.1.4 and later.

GuardAPI syntax

```
disable_auto_execute_suggested_dependencies parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|---|
| jobTrigger | String | Required. Guardium does not run the dependent tasks before running the specified task.. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To enable the job dependencies for the job userSynchronizationTrigger:

```
grdapi disable_auto_execute_suggested_dependencies jobTrigger=DataMartExtractionJobTrigger_5
ID=0
ok
```

Related concepts

- [Scheduling](#)
- [Job dependencies](#)

Related reference

- [Schedule and job dependencies APIs](#)

disable_big_data_interface

This command deactivates the active profile and removes its schedules, and optionally deletes the big data datasource definition and its metadata and reports. This command is valid for CM and standalone systems only.

This API is available in Guardium V10.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/bigDataInterface
```

GuardAPI syntax

```
disable_big_data_interface parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------------|------------|---|
| disable_readbac
k | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • 0 (false): Deactivates the current big data interface profile, and removes its schedules but does not delete the datasource definition or the reporting metadata. (Use this option if you want to subsequently re-enable the profile.) • 1 (true): Deletes the big data interface datasource definition and its schedules, and hides its metadata and reports. <p>Default = 0 (false)</p> |

Examples

Delete all definitions of the big data interface profile, its datasource and schedules, and hide its reports and metadata.

```
enable_big_data_interface disable_readback=1
```

Related concepts

- [Big Data Intelligence with data marts](#)

Related reference

- [Big Data Intelligence APIs](#)

disable_datastream

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/cloud_datasource
```

GuardAPI syntax

```
disable_datastream parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • <code>all_managed</code>: execute on all managed units but not the central manager • <code>all</code>: execute on all managed units and the central manager • <code>group:<group name></code>: execute on all managed units identified by <code><group name></code> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

disable_embed_eastern_font

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
disable_embed_eastern_font parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • <code>all_managed</code>: execute on all managed units but not the central manager • <code>all</code>: execute on all managed units and the central manager • <code>group:<group name></code>: execute on all managed units identified by <code><group name></code> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

disable_entitlement_optimization

This command disables the entitlement optimization feature on the local or specified units.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/disableEntitlementOptimization
```

GuardAPI syntax

```
disable_entitlement_optimization parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapi disable_entitlement_optimization
```

Related concepts

- [Entitlement Optimization](#)

Related reference

- [Entitlement optimization APIs](#)

disable_fam_crawler

This command disables the file activity monitor crawler. The file quick search activity and entitlement extractions scheduler are removed. This function also disables remote group population.

This API is available in Guardium V11.4, 11.5 and 12.0

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/disable_fam_crawler
```

GuardAPI syntax

```
disable_fam_crawler
```

Examples

To disable the FAM crawler

```
disable_fam_crawler
```

Related concepts

- [FAM discovery and classification in Windows and UNIX-Linux file servers](#)
- [Using rules for file activity policies](#)

Related reference

- [create_policy](#)
- [delete_policy](#)
- [enable_fam_crawler](#)
- [add_action_to_fam_rule](#)
- [create_fam_rule](#)
- [get_fam_crawler_info](#)

- [list_policy_fam_rule](#)
- [policy_fam_rule_delete](#)

disable_health_analyzer

This command disables the disk and database health analyzer.

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/disableHealthAnalyzer
```

GuardAPI syntax

```
disable_health_analyzer parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Use this command to disable the disk and database health analyzer:

```
grdapicl disable_health_analyzer
```

Related reference

- [Health analyzer APIs](#)

disable_ip_to_host_aliases

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/disable_ip_host_alias
```

GuardAPI syntax

```
disable_ip_to_host_aliases parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

disable_monitoring_ranger_service

Use this command to disable a Ranger service (Hadoop monitoring).

This command requires valid administrative authority on the Ambari server such as an admin or service administrator account. After running the command, the Ambari administrator must restart the affected Hadoop components so that the changes take effect.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/disable_monitoring_ranger_service
```

GuardAPI syntax

```
disable_monitoring_ranger_service parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| clusterName | String | Required. Ambari cluster name. |
| serviceName | String | Required. Name of the service. Valid values: <ul style="list-style-type: none"> • hdfs • hive • hbase • kafka • solr • storm |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To disable monitoring on the Cluster4 HDFS service:

```
grdapi disable_monitoring_ranger_service clusterName=Cluster4 serviceName=HDFS
```

System response:

ID=0

The Hadoop service configuration has been changed. Ask the Hadoop administrator to restart the Hadoop service to activate the change.
HDFS Monitoring Disabled on <server name>:5565

Related concepts

- [Hadoop integration using Hortonworks and Apache Ranger](#)

Related reference

- [Hadoop monitoring APIs](#)
 - [S-TAP Hadoop parameters](#)
-

disable_native_audit

This API disables DB Audit (native audit) on the specified cloud datasource.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/disable_native_audit
```

GuardAPI syntax

```
disable_native_audit parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| datasource_name | String | Required. A cloud datasource defined in Guardium. |
| should_restart | Boolean | Valid values: <ul style="list-style-type: none"> • 0 (false) • 1 (true) Default = 0 (false) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Related tasks

- [Cloud database service protection with native audit](#)

Related reference

- [Native audit APIs](#)
-

disable_outliers_detection

Run this command on a standalone system, or on a central manager.

The command affects the Guardium systems differently, depending on their setup.

Single CM environment

Run on a CM to disable outliers detection on all managed units registered with the CM, by running the API command with no additional parameters. You can limit the disable to a list of units.

When disabling on a collector, if this is the only collector sending data to the aggregator, then the collector stops sending data, and outliers detection is disabled on the aggregator.

Multi-CM environment

Run on a CM with no additional parameters, to disable outliers detection on all managed units registered to the CM. You can limit the disable to a list of units.

To disable on individual aggregators or collectors, use the commands [disable_outliers_detection_cross_cm_agg](#) and [disable_outliers_detection_cross_cm_collector](#).

Single Collector

Run the command on a collector that does not extract data to an aggregator, to disable it locally.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/disableOutliersDetection
```

GuardAPI syntax

```
disable_outliers_detection parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------------|------------|---|
| managed_units_hostnames | String | Specific managed units on which the command is executed. Optional when running the API on the CM. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Run this command on the CM to disable the outliers detection on all the units under the CM and on all units registered to the CM thereafter:

```
grdapicl disable_outliers_detection
```

Related tasks

- [Enabling and disabling outliers detection](#)

Related reference

- [Outliers detection APIs](#)

disable_outliers_detection_agg

Run this API on a central manager to disable outliers detection on the specified aggregator.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/disableOutliersDetectionOnAgg
```

GuardAPI syntax

```
disable_outliers_detection_agg parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------------|------------|--|
| aggregator_host_name | String | Required. The specific aggregator disabled for outliers detection. |

Examples

Run this command to disable outliers detection on the aggregator **agg-sw**:

```
disable_outliers_detection_agg aggregator_host_name=agg-sw
```

Related concepts

- [Outliers detection](#)

Related tasks

- [Enabling and disabling outliers detection](#)

Related reference

- [Outliers detection APIs](#)

disable_outliers_detection_cross_cm_agg

Run on a central manager to disable outliers on the collector(s) that send data to the specified aggregator(s). This is for use in a multi-central manager environment; the aggregator is in this central manager's environment but the collectors are managed by a different central manager.

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/disableOutliersDetectionOnAggCrossCm
```

GuardAPI syntax

```
disable_outliers_detection_cross_cm_agg parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------------|------------|---|
| aggregator_host_name | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To disable outliers on the collectors that send data to the aggregator **agg12**, run this command on the CM that the aggregator **agg12** reports to:

```
disable_outliers_detection_cross_cm_agg aggregator_host_name=agg12
```

Related tasks

- [Enabling and disabling outliers detection](#)

Related reference

- [Outliers detection APIs](#)

disable_outliers_detection_cross_cm_collector

Run on a central manager to disable outliers on the specified collector(s) in this central manager's environment. This is for use in a multi-central manager environment; the collector is in this central manager's environment but the data is sent to an aggregator in another central manager's environment.

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/disableOutliersDetectionOnCollectorsCrossCM
```

GuardAPI syntax

```
disable_outliers_detection_cross_cm_collector parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------------|------------|---|
| collector_host_names | String | Required. Comma-separated list of collector names. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To disable outliers detection on the collectors `coll1a`, `coll2a`, run this command on the central manager of the collectors:

```
disable_outliers_detection_cross_cm_collector collector_host_names=coll1a,coll2a
```

Related concepts

- [Outliers detection](#)

Related reference

- [Outliers detection APIs](#)

disable_persistent_queue_universal_connector

Run this API to disable a Persistent Queue on Logstash inputs. Changes take effect only after reloading the configurations or restarting Logstash.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/disablePersistentQueue
```

GuardAPI syntax

```
disable_persistent_queue_universal_connector parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To disable on the current Guardium system:

```
grdapi disable_persistent_queue_universal_connector
Guardium Universal Connector command has been executed.
```

Related concepts

- [Guardium universal connector](#)

Related reference

- [Guardium universal connector APIs](#)

disable_policy_analyzer

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/disable_policy_analyzer
```

GuardAPI syntax

```
disable_policy_analyzer parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

disable_purge

Use this command to disable the scheduled purge for one or more Guardium® systems.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `DELETE` method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/disable_purge
```

GuardAPI syntax

```
disable_purge parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To disable the scheduled purge on the system on which you enter the command:

```
grdapi disable_purge
```

Related tasks

- [Managing stored data](#)

Related reference

- [Archive, export, import, purge, and restore APIs](#)

disable_quick_search

This command disables investigation dashboard functionality.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/disable_quick_search
```

GuardAPI syntax

```
disable_quick_search parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| all | Boolean | <p>In an environment with a Central Manager, use this parameter to disable search on all managed units. Valid values:</p> <ul style="list-style-type: none">• 0 (false): Disable only on the unit where the command is executed.• 1 (true): Disable on all managed units. <p>Default = 0 (false)</p> |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To disable quick search on the current unit and all of its managed units:

```
disable_quick_search all=true
```

Related concepts

- [Big Data Intelligence with data marts](#)

Related reference

- [Data mart APIs](#)
- [Investigation dashboard APIs](#)

disable_riskspotter

Run this command on a central manager to disable RiskSpotter on all of the central manager's managed units, or on a stand-alone Guardium system.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/disable_riskspotter
```

GuardAPI syntax

```
disable_riskspotter
```

This API takes no parameters.

Examples

Run this command on a central manager to disable RiskSpotter on all of its managed units:

```
grdapicl disable_riskspotter
```

Related concepts

- [Risk Spotter](#)

disable_special_attributes

This API removes access for non-admin users to view attributes for certain groups in Query-Report Builder.

Within Query-Report Builder, admin users can see all attributes while non-admin users can view only query attributes, except attributes that are designated as admin only (such as IDs). Use `disable_special_attributes` to disallow non-admin users to view all of the attributes within a specified `attributesGroup`.

Note: When an attribute group is disabled, all of the attributes within that group are unavailable to non-admin users.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
disable_special_attributes parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| attributesGroup | String | Required. Valid values: <ul style="list-style-type: none">• <i>data set</i>• <i>ims</i>• <i>hive</i>• <i>apex</i>• <i>mapreduce</i>• <i>bi</i>• <i>ims/data set</i>• <i>f5</i>• <i>db2 i</i> |

Examples

The following example disables Hive attributes for all non-admin users:

```
grdapi disable_special_attributes attributesGroup=hive
```

Sample output

```
> grdapi enable_special_attributes attributesGroup=hive
Following Attributes have been Disabled: Hive Parsed SQL, Hive User, Hive Command, Hive Database,
Hive Table Name, Hive Error
ok
```

Related reference

- [enable_special_attributes](#)

disable_test_result_detail_string_setting

Use this API command to disable writing detailed test results of a vulnerability assessment into the Test Result entity.

This API is available in Guardium V11.4 and later.

This API takes no parameters.

For backward compatibility, Vulnerability Assessment (VA) continues to store all detailed test results in one record in addition to creating a separate record for each detailed finding. The API command **disable_test_result_detail_string_setting** disables the writing all detailed test findings into one record.

Important: After you run this API command, you cannot re-enable writing all detailed test results into the Test Result entity. However, VA continues to create a separate record for each detailed finding. When the test results are exported to an external location, you can normalize each detailed finding into a record of its own.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/detail_string_setting
```

GuardAPI syntax

```
disable_test_result_detail_string_setting
```

Example

```
grdapi disable_test_result_detail_string_setting
ID=0
Test details are written only to the TEST_RESULT_DETAIL table.
ok
```

Related reference

- [Assessment APIs](#)

disable_threat_detection_use_case

Use this command to remove use case types from the threat detection analysis.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/disable_threat_detection_use_case
```

GuardAPI syntax

```
disable_threat_detection_use_case parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| case_name | String | Required. For valid values, call disable_threat_detection_use_case from the command line with --help=true. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">all_managed: execute on all managed units but not the central managerall: execute on all managed units and the central managergroup:<group name>: execute on all managed units identified by <group name>host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To remove the grants use case from the threat detection analysis:

```
grdapi disable_threat_detection_use_case case_name=GRANTS
```

Related concepts

- [Threat detection analytics](#)

Related reference

- [Threat detection analytics APIs](#)

disable_threat_finder

Run this command on a CM or on a standalone unit to disable the threat finder functionality of the Active threat analytics.

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/disable_threat_finder
```

GuardAPI syntax

```
disable_threat_finder parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To disable threat finder on the standalone unit or on the CM environment:

```
grdapi disable_threat_finder
ID=0
ok
```

Related concepts

- [Advanced threat analytics](#)

Related reference

- [Threat detection analytics APIs](#)

discover_streams

This API returns the number of AWS data streams for the specified cloud DB service account (cloudTitle) and region.

To find details about a stream, use the [get_streams](#) API.

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/discover_datastream
```

GuardAPI syntax

```
discover_streams parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| cloudTitle | String | <p>Required. The name of the cloud DB service account. For valid values, call <code>discover_streams</code> from the command line with <code>--help=true</code>.
For more information, see Define, modify, and delete AWS cloud DB service accounts.</p> |
| regions | String | Requires for AWS only. For valid values, call <code>discover_streams</code> from the command line with <code>--help=true</code> . |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapi discover_streams cloudTitle=mytest-aws regions=us-east-1
```

Sample output:

```
ID=0
Number of Streams discovered for the given cloud Account: 3
ok
```

Related tasks

- [Discover and configure AWS data streams](#)

Related reference

- [get_streams](#)

display_external_stap_config

This API displays the values of specified External S-TAP® parameters. You can also display all modifiable External S-TAP parameters.

Use [update_external_stap_config](#) to change the value of External S-TAP parameters. External S-TAPs are supported on UNIX or Linux machines only.

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/display_external_stap_config
```

GuardAPI syntax

```
display_external_stap_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|----------------------|------------|--|
| filterConfigByParams | String | <p>Use this parameter to specify the specific parameters you want to output. Comma separated string of one or more of these valid values:</p> <ul style="list-style-type: none"> • all <p>TAP section:</p> <ul style="list-style-type: none"> • <i>add_to_verification_schedule</i> • <i>all_can_control</i> • <i>alternate_ips</i> • <i>appserver_installed</i> • <i>appserver_login_pattern</i> • <i>appserver_ports</i> • <i>appserver_session_pattern</i> • <i>appserver_session_postfix</i> • <i>appserver_session_prefix</i> • <i>appserver_username_postfix</i> • <i>appserver_username_prefix</i> • <i>appserver_usersess_pattern</i> • <i>appserver_usersess_postfix</i> • <i>appserver_usersess_prefix</i> • <i>bad_alloc_counter_max</i> • <i>buf_msg_time_interval</i> • <i>buffer_file_size</i> • <i>buffer_mmap_file</i> • <i>checksum</i> • <i>checksum_configuration</i> • <i>compression_level</i> • <i>connection_timeout_sec</i> • <i>db_exit_list</i> • <i>db_ignore_response</i> • <i>db_ignore_response_bypass_bytes</i> • <i>db_ignore_response_filter</i> • <i>db_ignore_response_resets_per_request</i> • <i>db_request_handler_enable</i> • <i>enable_dynamic_ring_buffers</i> • <i>extra_info</i> • <i>failover_tls</i> • <i>firewall_default_state</i> • <i>firewall_fail_close</i> • <i>firewall_force_unwatch</i> • <i>firewall_force_watch</i> • <i>firewall_installed</i> • <i>firewall_timeout</i> • <i>force_server_ip</i> • <i>guardium_ca_path</i> • <i>guardium_crl_path</i> • <i>kerberos_plugin_dir</i> • <i>load_balancer_ip</i> • <i>load_balancer_load_affinity</i> • <i>max_server_write_size</i> • <i>min_bytes_to_compress</i> • <i>modification_count</i> • <i>modification_host</i> • <i>modification_microsec</i> • <i>msg_aggregate_timeout</i> • <i>msg_count_watermark</i> • <i>participate_in_load_balancing</i> • <i>private_tap_ip</i> • <i>qrw_default_state</i> • <i>qrw_force_unwatch</i> • <i>qrw_force_watch</i> • <i>qrw_installed</i> • <i>remote_messages</i> • <i>sqlguard_cert_cn</i> • <i>stap_statistic</i> • <i>stap_statistic_version</i> • <i>syslog_messages</i> • <i>tap_buf_dir</i> • <i>tap_debug_output_level</i> • <i>tap_failover_session_quiesce</i> • <i>tap_failover_session_size</i> • <i>tap_identifier</i> • <i>tap_ip</i> • <i>tap_log_dir</i> • <i>upload_feature</i> |

| Parameter | Value type | Description |
|-----------------|------------|--|
| stapHost | String | <p>Required. Can be one of:</p> <ul style="list-style-type: none"> The UUID of the External S-TAP. <i>all_active</i>: All External S-TAPs that are configured to report to this Guardium system. <p>For valid values, call <code>display_external_stap_config</code> from the command line with <code>--help=true</code>.</p> |
| api_target_host | String | <p>Required when running on a central manager.</p> <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> <i>all_managed</i>: execute on all managed units but not the central manager <i>all</i>: execute on all managed units and the central manager <i>group:<group name></i>: execute on all managed units identified by <i><group name></i> host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GRDAPI examples

```
>grdapi display_external_stap_config --help=true
>grdapi display_stap_config stapHost=all_active filterConfigByParams=db_user
```

Related reference

- [display_stap_config](#)
- [update_external_stap_config](#)

display_stap_config

This command outputs the properties of all S-TAPs, including the inspection engines and SQL connections, on the specified host. Optionally, specify the S-TAP® parameters you want to output.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/display_stap_config
```

GuardAPI syntax

```
display_stap_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------------|------------|---|
| filterConfigByParams | String | <p>Use this parameter to specify the specific parameters you want to output. Comma separated string of one or more of these valid values:</p> <ul style="list-style-type: none"> <i>all</i> <p>TAP section:</p> <ul style="list-style-type: none"> <i>add_to_verification_schedule</i> (UNIX, Windows) <i>alert_on_shared_memory_enabling</i> (Windows) <i>all_can_control</i> (UNIX, Windows) <i>alternate_ips</i> (UNIX, Windows) <i>appserver_installed</i> (UNIX, Windows) <i>appserver_login_pattern</i> (UNIX, Windows) <i>appserver_ports</i> (UNIX, Windows) <i>appserver_session_pattern</i> (UNIX, Windows) <i>appserver_session_postfix</i> (UNIX, Windows) <i>appserver_session_prefix</i> (UNIX, Windows) <i>appserver_username_postfix</i> (UNIX, Windows) <i>appserver_username_prefix</i> (UNIX, Windows) <i>appserver_usersess_pattern</i> (UNIX, Windows) <i>appserver_usersess_postfix</i> (UNIX, Windows) <i>appserver_usersess_prefix</i> (UNIX, Windows) |

| Parameter | Value type | Description |
|-----------|------------|---|
| | | <ul style="list-style-type: none"> • <i>atap_exec_location</i> (UNIX) • <i>auto_discovery</i> (Windows) • <i>bad_alloc_counter_max</i> (UNIX) • <i>buf_msg_time_interval</i> (UNIX, Windows) • <i>buffer_file_size</i> (UNIX, Windows) • <i>buffer_mmap_file</i> (UNIX, Windows) • <i>buffer_percentage_for_priority_packet</i> (UNIX) • <i>cas_checkpoint_period</i> (UNIX, Windows) • <i>cas_client_baseline</i> (UNIX, Windows) • <i>cas_client_checkpoint</i> (UNIX, Windows) • <i>cas_fail_over_file</i> (UNIX, Windows) • <i>cas_fail_over_file_size_limit</i> (Windows) • <i>cas_max_reconnect_attempts</i> (UNIX, Windows) • <i>cas_md5_size_limit</i> (UNIX, Windows) • <i>cas_raw_data_limit</i> (UNIX, Windows) • <i>cas_reconnect_interval</i> (UNIX, Windows) • <i>cas_task_baseline</i> (UNIX, Windows) • <i>cas_task_checkpoint</i> (UNIX, Windows) • <i>cassandra_audit_delimiter</i> (UNIX) • <i>cassandra_audit_enabled</i> (UNIX) • <i>checksum</i> (UNIX, Windows) • <i>checksum_configuration</i> (UNIX, Windows) • <i>compression_level</i> (UNIX, Windows) • <i>connection_timeout_sec</i> (UNIX, Windows, i) • <i>correlation_timeout</i> (Windows) • <i>db_exit_list</i> (UNIX) • <i>db2_shmem_driver_installed</i> (Windows) • <i>db2_tap_installed</i> (Windows) • <i>db_ignore_response</i> (UNIX, Windows) • <i>db_ignore_response_bypass_bytes</i> (UNIX, Windows) • <i>db_ignore_response_filter</i> (UNIX, Windows) • <i>db_ignore_response_local</i> (UNIX, Windows) • <i>db_ignore_response_resets_per_request</i> (UNIX, Windows) • <i>db_request_handler_enable</i> (UNIX) • <i>devices</i> (UNIX, Windows) • <i>disable_shared_memory_if_turned_on</i> (Windows) • <i>discovery_debug</i> (UNIX) • <i>discovery_interval</i> (UNIX, Windows). Valid values: <n>m (for minutes) and <n>h (for hours). • <i>enable_dynamic_ring_buffers</i> (UNIX) • <i>extra_info</i> (UNIX, Windows) • <i>failover_tls</i> (UNIX, Windows,i) • <i>fam_enable</i> (UNIX, Windows) • <i>firewall_default_state</i> (UNIX, Windows) • <i>firewall_fail_close</i> (UNIX, Windows) • <i>firewall_force_unwatch</i> (UNIX, Windows) • <i>firewall_force_watch</i> (UNIX, Windows) • <i>firewall_installed</i> (UNIX, Windows) • <i>firewall_timeout</i> (UNIX, Windows) • <i>force_server_ip</i> (UNIX) • <i>guardium_ca_path</i> (UNIX) • <i>guardium_crl_path</i> (UNIX) • <i>hunter_trace</i> (UNIX) • <i>kafka_bootstrap_servers</i> (UNIX) • <i>kafka_keytab</i> (UNIX) • <i>kafka_principal</i> (UNIX) • <i>kafka_reader_enabled</i> (UNIX) • <i>kafka_topic_name</i> (UNIX) • <i>kafka_use_tls</i> (UNIX) • <i>kerberos_plugin_dir</i> (UNIX) • <i>khash_max_entries</i> (UNIX) • <i>khash_table_length</i> (UNIX) • <i>krb_mssql_driver_installed</i> (Windows) • <i>krb_mssql_driver_nonblocking</i> (Windows) • <i>krb_mssql_driver_ondemand</i> (Windows) • <i>krb_mssql_driver_user_collect_time</i> (UNIX, Windows) • <i>ktap_buffer_flush</i> (UNIX) • <i>ktap_buffer_size</i> (UNIX) • <i>ktap_dbgev_ev_list</i> (UNIX) • <i>ktap_dbgev_func_name</i> (UNIX) • <i>ktap_fast_file_verdict</i> (UNIX) • <i>ktap_fast_tcp_verdict</i> (UNIX) • <i>ktap_installed</i> (UNIX) • <i>ktap_request_timeout</i> (UNIX) • <i>lhmon_driver_installed</i> (Windows) • <i>lhmon_for_network</i> (Windows) • <i>load_balancer_ip</i> (UNIX, Windows) • <i>load_balancer_load_affinity</i> (UNIX) • <i>load_balancer_num_mus</i> (UNIX, Windows) |

| Parameter | Value type | Description |
|-----------|------------|--|
| | | <ul style="list-style-type: none"> • <i>log4j_listen_address</i> (UNIX) • <i>log4j_num_connections</i> (UNIX) • <i>log4j_port</i> (UNIX, Windows) • <i>log4j_reader_enabled</i> (UNIX) • <i>log_program_name</i> (UNIX) • <i>max_server_write_size</i> (UNIX) • <i>min_bytes_to_compress</i> (UNIX, Windows) • <i>modification_count</i> (UNIX, Windows) • <i>modification_host</i> (UNIX, Windows) • <i>modification_microsec</i> (UNIX, Windows) • <i>msg_aggregate_timeout</i> (UNIX) • <i>msg_count_watermark</i> (UNIX) • <i>named_pipes_driver_installed</i> (Windows) • <i>network_namedpipes</i> (Windows) • <i>number_of_processors</i> (Windows) • <i>ora_driver_installed</i> (Windows) • <i>participate_in_load_balancing</i> (UNIX, Windows,i) • <i>pcap_backup_ktap</i> (UNIX, Windows) • <i>pcap_buffer_size</i> (UNIX) • <i>pcap_dispatch_count</i> (UNIX) • <i>pcap_read_timeout</i> (UNIX) • <i>private_tap_ip</i> (UNIX) • <i>qrw_default_state</i> (UNIX) • <i>qrw_force_unwatch</i> (UNIX) • <i>qrw_force_watch</i> (UNIX) • <i>qrw_installed</i> (UNIX) • <i>remote_messages</i> (UNIX, Windows,i) • <i>shared_memory_driver_installed</i> (Windows) • <i>sqlguard_cert_cn</i> (UNIX) • <i>stap_statistic</i> (UNIX) • <i>stap_statistic_version</i> (UNIX, Windows) • <i>sybase_driver_installed</i> (Windows) • <i>syslog_messages</i> (UNIX, Windows) • <i>tap_buf_dir</i> (UNIX) • <i>tap_debug_output_level</i> (UNIX) • <i>tap_failover_session_quiesce</i> (UNIX) • <i>tap_failover_session_size</i> (UNIX) • <i>tap_identifier</i> (UNIX, Windows) • <i>tap_ip</i> (UNIX, Windows) • <i>tap_log_dir</i> (UNIX) • <i>tap_run_as_root</i> (UNIX) • <i>tee_installed</i> (UNIX) • <i>tee_msg_buf_len</i> (UNIX) • <i>tracefiles_dir</i> (Windows) • <i>uid_chain_sshd_ip</i> (UNIX) • <i>upload_feature</i> (UNIX, Windows) • <i>use_tls</i> (UNIX, Windows,i) • <i>wait_for_db_exec</i> (UNIX) <p>DB section:</p> <ul style="list-style-type: none"> • <i>connect_to_ip</i> (UNIX) • <i>db2_client_offset</i> (UNIX, Windows) • <i>db2_fix_pack_adjustment</i> (UNIX, Windows) • <i>db_exec_file</i> (UNIX) • <i>db_install_dir</i> (UNIX) • <i>db_user</i> (UNIX) • <i>db_version</i> (UNIX, Windows) • <i>encryption</i> (UNIX) • <i>exclude_networks</i> (UNIX, Windows) • <i>instance_name</i> (Windows) • <i>intercept_types</i> (UNIX) • <i>named_pipe</i> (Windows) • <i>networks</i> (UNIX, Windows) • <i>port_range_end</i> (UNIX, Windows) • <i>port_range_start</i> (UNIX, Windows) • <i>priority_count</i> (UNIX, Windows) • <i>real_db_port</i> (UNIX, Windows) • <i>tap_db_process_names</i> (Windows) • <i>unix_domain_socket_marker</i> (UNIX) <p>SQLGUARD section:</p> <ul style="list-style-type: none"> • <i>connection_pool_size</i> (UNIX) • <i>num_main_thread</i> (UNIX) • <i>sqlguard_ip</i> (UNIX, Windows, i) <p>SQLC_n section (UNIX Oracle Unified Auditing only):</p> <ul style="list-style-type: none"> • <i>data_pull_interval</i> (UNIX) |

| Parameter | Value type | Description |
|-----------------|------------|---|
| | | <ul style="list-style-type: none"> • <i>instance</i> (UNIX) • <i>username</i> (UNIX) • <i>roles</i> (UNIX) • <i>data_pull_num_rows</i> (UNIX) <p>Default = all</p> |
| stapHost | String | <p>Required. Valid values:</p> <ul style="list-style-type: none"> • <i>all_active</i>: All S-TAPs that are configured to report to this Guardium® system • <i>all_unix_active</i>: All S-TAPs that are configured to report to this Guardium system and are running on Linux-UNIX servers. • <i>all_windows_active</i>: All S-TAPs that are configured to report to this Guardium system and are running on Windows servers. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • <i>all_managed</i>: execute on all managed units but not the central manager • <i>all</i>: execute on all managed units and the central manager • <i>group:<group name></i>: execute on all managed units identified by <i><group name></i> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <i>api_target_host=10.0.1.123</i>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <i>api_target_host=10.0.1.123</i>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To view the full S-TAP configuration:

```
grdapic display_stap_config stapHost=all_active filterConfigByParams=all
```

Sample response:

```
ID=9
1. 9.42.29.158
Id:9
TAP:
add_to_verification_schedule=0
all_can_control=0
alternate_ips=
appserver_installed=0
appserver_login_pattern=X
appserver_ports=8080
appserver_session_pattern=X
appserver_session_postfix=X
appserver_session_prefix=X
appserver_username_postfix=X
appserver_username_prefix=X
appserver_usersess_pattern=X
appserver_usersess_postfix=X
appserver_usersess_prefix=X
atap_exec_location=/var/guard
atap_request_handler_enable=1
buffer_file_size=50
cas_checkpoint_period=3600
cas_client_baseline=client_baseline
cas_client_checkpoint=client_checkpoint
cas_fail_over_file=fail_over_file
cas_max_reconnect_attempts=5000
cas_md5_size_limit=1000
cas_raw_data_limit=1000
cas_reconnect_interval=60
cas_task_baseline=task_baseline
cas_task_checkpoint=task_checkpoint
cassandra_audit_delimiter=GUARD_DELIM
cassandra_audit_enabled=0
connection_timeout_sec=10
db_ignore_response=none
db_ignore_response_bypass_bytes=4096
db_ignore_response_filter=0.0.0.0/0.0.0.0
db_ignore_response_local=1
db_ignore_response_resets_per_request=0
devices=none
discovery_dbs=oracle:db2:informix:mysql:postgres:sybase:hadoop:teradata:netezza:memsql
discovery_debug=0
discovery_interval=24h
discovery_ora_alt_locations=
discovery_port=8443
failover_tls=1
fam_enable=0
firewall_default_state=0
firewall_fail_close=0
firewall_force_unwatch=
firewall_force_watch=
firewall_installed=0
firewall_timeout=10
```

```

force_log_limited=0
force_server_ip=0
fsm_driver_installed=0
guardium_ca_path=
guardium_crl_path=
hunter_trace=0
kafka_bootstrap_servers=
kafka_group_name=stap
kafka_is_mapr=0
kafka_keytab=
kafka_principal=
kafka_reader_enabled=0
kafka_ssl_ca_location=
kafka_topic_name=NavigatorAuditEvents
kafka_use_tls=0
kerberos_plugin_dir=
khash_max_entries=8192
khash_table_length=24593
ktap_buffer_flush=0
ktap_buffer_size=4194304
ktap_dbgev_ev_list=0
ktap_dbgev_func_name=all
ktap_fast_file_verdict=1
ktap_fast_tcp_verdict=1
ktap_installed=0
ktap_request_timeout=5
ktap_version=
ld_library_paths=
load_balancer_ip=
load_balancer_num_mus=1
log4j_listen_address=0.0.0.0
log4j_num_connections=20
log4j_reader_enabled=0
log_program_name=0
max_packet_num=2000
max_server_write_size=65536
msg_aggregate_timeout=100
msg_count_watermark=64
os_type=
participate_in_load_balancing=2
pcap_buffer_size=-1
pcap_dispatch_count=16
pcap_read_timeout=0
private_tap_ip
qrw_default_state=0
qrw_force_unwatch=
qrw_force_watch=
qrw_installed=0
remote_messages=1
sqlc_properties_dir=
sqlguard_cert_cn=
stap_statistic=0
syslog_messages=1
tap_buf_dir=
tap_debug_output_level=0
tap_failover_session_quiesce=240
tap_failover_session_size=1024
tap_ip=9.42.29.158
tap_log_dir=
tap_run_as_root=1
tap_type=stap
tap_version=STAP-11.1.0.0_r106678_trunk_1-20190519_1933
tee_installed=0
tee_msg_buf_len=128
uid_chain_sshd_ip=0
upload_feature=1
use_tls=0
wait_for_db_exec=1

DB_0:
connect_to_ip=127.0.0.1,::1
db2_fix_pack_adjustment=20
db2_shmem_client_position=0
db2_shmem_size=131072
db2bp_path=NULL
db_exec_file=/$ORACLE_HOME/bin/oracle
db_install_dir=/home/oracle18
db_type=oracle
db_user=oracle18
encryption=0
db_version=18
instance_running=1
intercept_types=NULL
load_balanced=1
port_range_end=1525
port_range_start=1520
priority_count=20
real_db_port=1521
tap_identifier=oracle_9.70.147.74(1521,1521,DB_0)
tee_listen_port=0
unix_domain_socket_marker=ORCL
networks=0.0.0.0/0.0.0.0,::/0
exclude_networks=

```

```

DB_1:
protocol=mysql
connect_to_ip=127.0.0.1
db2_fix_pack_adjustment=20
db2_shmem_client_position=0
db2_shmem_size=131072
db2bp_path=
db_exec_file=/home/mysql57/mysql/bin/
db_install_dir=/home/mysql57/mysql/data
db_type=mysql
db_user=mysql57
encryption=0
exclude_networks=
informix_version=9
instance_running=1
intercept_types=
load_balanced=1
networks=0.0.0.0/0.0.0.0
port_range_end=33060
port_range_start=3357
priority_count=20
real_db_port=3357
tap_identifier=mysql_9.42.29.158(3357,33060,DB_2)
tee_listen_port=
unix_domain_socket_marker=mysql.sock

DB_2:
protocol=db2
connect_to_ip=127.0.0.1
db2_fix_pack_adjustment=20
db2_shmem_client_position=61440
db2_shmem_size=131072
db2bp_path=
db_exec_file=/home/db2inst1/sqllib/adm/db2sysc
db_install_dir=/home/db2inst1
db_type=db2
db_user=db2inst1
encryption=0
exclude_networks=
informix_version=9
instance_running=1
intercept_types=
load_balanced=1
networks=0.0.0.0/0.0.0.0
port_range_end=50000
port_range_start=50000
priority_count=20
real_db_port=50000
tap_identifier=db2_9.42.29.158(50000,50000,DB_3)
tee_listen_port=
unix_domain_socket_marker=

SQLGUARD_0:
connection_pool_size=0
num_main_thread=1
primary=1
sqlguard_ip=<Guardium host-0 IP or name>
sqlguard_port=16016

SQLGUARD_1:
connection_pool_size=0
num_main_thread=1
primary=2
sqlguard_ip=<Guardium host-1 IP or name>
sqlguard_port=16016

SQLGUARD_2:
connection_pool_size=0
num_main_thread=1
primary=3
sqlguard_ip=<Guardium host-2 IP or name>
sqlguard_port=16016

SQLGUARD_3:
connection_pool_size=0
num_main_thread=1
primary=4
sqlguard_ip=<Guardium host-3 IP or name>
sqlguard_port=16016

SQLGUARD_4:
connection_pool_size=0
num_main_thread=1
primary=5
sqlguard_ip=<Guardium host-4 IP or name>
sqlguard_port=16016

SQLGUARD_5:
connection_pool_size=0
num_main_thread=1
primary=6
sqlguard_ip=<Guardium host-5 IP or name>
sqlguard_port=16016
ok

```

To view only the S-TAP parameters db_user and sqlguard_port:

```
grdapi display_stap_config stapHost=all_active filterConfigByParams=db_user,sqlguard_port
```

Sample response:

```
1. <S-TAP host IP>
Id:22

DB_0:
protocol=db2
db_user=db2inst1

DB_1:
protocol=Mysql
db_user=mysql8

DB_2:
protocol=Mysql
db_user=mysql8

DB_3:
protocol=Mysql
db_user=mysql157

SQLGUARD_0:
sqlguard_port=16016

SQLGUARD_1:
sqlguard_port=16016

SQLGUARD_2:
sqlguard_port=16016

2. <S-TAP host IP>
Id:21

DB_0:
protocol=db2
db_user=db2inst1

DB_1:
protocol=Mysql
db_user=mysql57

DB_2:
protocol=Mysql
db_user=mysql57

SQLGUARD_0:
sqlguard_port=16016

SQLGUARD_1:
sqlguard_port=16016

SQLGUARD_2:
sqlguard_port=16016

SQLGUARD_3:
sqlguard_port=16016
ok
```

Related reference

- [S-TAP and inspection engine APIs](#)

edit.kafka.cluster

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/kafka_cluster
```

GuardAPI syntax

```
edit.kafka.cluster parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-------------|------------|--|
| action | String | Valid values: <ul style="list-style-type: none">• add• delete |
| clusterName | String | For valid values, call edit_kafka_cluster from the command line with --help=true. |
| memberList | String | For valid values, call edit_kafka_cluster from the command line with --help=true. |

enable_advanced_threat_scanning

This command enables the threat detection analytics processes to check for specific database attacks such as SQL injection and malicious stored procedures.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/enable_advanced_threat_scanning
```

GuardAPI syntax

```
enable_advanced_threat_scanning parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| all | Boolean | In a central management configuration only, enables all threat detection scanners on all managed units. This is equivalent to the "all" option for the parameter <code>api_target_host</code> . Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| schedule_start | Date | Specifies the date and time to start running the processes, in the format yyyy-mm-dd hh:mm:ss (24-hour clock). |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To enable advanced threat analytics:

```
grdapi enable_advanced_threat_scanning all=true schedule_start="2016-03-24 12:00:05"
```

If threat analytics is enabled, but outlier detection is not enabled, the system responds:

```
Warning - Enabling advance threat scanning (AKA Eagle Eye) when Analytic anomaly detection is disabled.  
Advance threat scanning (AKA Eagle Eye) enabled.  
ok
```

Related concepts

- [Threat Detection Analytics](#)

Related reference

- [Threat detection analytics APIs](#)

enable_all_tls

Enables all versions of TLS (TLS 1.2 and TLS 1.3) on either the current system or on all associated managed units.

After you disable TLS 1.2 (with [enable_latest_tls](#)), you might find that you need to re-enable it. Use this API to add TLS 1.2 back to your Guardium configuration.

Tip: This API takes a few minutes to run.

This API is available in Guardium v12.0 and later.

GuardAPI syntax

```
enable_all_tls parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| all | Boolean | <p>Required. For a central manager, select whether to enable TLS 1.2 and TLS 1.3 on all associated managed units. Valid values:</p> <ul style="list-style-type: none">• 0 (false) - Enable TLS 1.2 and TLS 1.3 on this machine only.• 1 (true) - Enable TLS 1.2 and TLS 1.3 on this machine and associated managed units. <p>Default = 0 (false)</p> |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related tasks

- [Managing the TLS version](#)

Related reference

- [enable_latest_tls](#)
- [get_secured_protocols_info](#)

Related information

- [show_tls_enabled](#)

enable_big_data_interface

This command specifies the active profiles and schedule of the big data interface, activates extraction of all data marts in the profile according to the unit types, and defines the Big Data collection as a datasource.

This command can run on a central manager or standalone unit. You can define only one interface per Guardium® system.

This API is available in Guardium V10.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/bigDataInterface
```

GuardAPI syntax

```
enable_big_data_interface parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|---|
| ds_desc | String | Datasource description. Default is Big Data Intelligence. |
| ds_host | String | Required. Hostname of Big Data storage place, from which data is pulled to Guardium for reports, monitoring, and so on. |
| ds_password | String | Required. Password for ds_user, which pulls Big Data from the datasource. |
| ds_port | Integer | Port via which Guardium pulls Big Data from the datasource. Default = 27117. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| ds_user | String | Required. User that pulls Big Data from the datasource. This user can be different from the target user. |
| profile_name | String | Required. Name of datamart extraction profile, either a default profile or a profile defined by add_dm_to_profile or clone_extraction_profile . For a list of the profiles, run grdapi get_extraction_profile_info . For valid values, call enable_big_data_interface from the command line with --help=true . |
| start_date | Date | When to start sending data to the Big Data datasource. Format is one of: <ul style="list-style-type: none"> • NOW -<n> <minute hour day week month • yyyy-mm-dd hh:mm:ss Default = time at which the command is executed. |
| target_host | String | Target data host for extracted data marts. This is usually the same as the ds_host. If you require a staging area before moving data to the host, then target_host is not the same as ds_host. |
| target_password | String | Password for target_user, or key pair authentication file. If left blank, defaults to ds_password. When using a key file, the syntax is fileName=<path/filename> |
| target_path | String | Target folder location for extracted data marts. Default = /local/raid0/sonargd/incoming. |
| target_port | Integer | Port on the target server. Default = 22 (SCP). |
| target_user | String | User for the target_host. If left blank, defaults to ds_user. |
| unit_group | String | Enables data export from the CM or the group's managed units. Default = ALL
For valid values, call enable_big_data_interface from the command line with --help=true . |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

Enable the big data export profile for the Basic Summary data mart on the specified host.

```
enable_big_data_interface ds_host=<hostname> ds_user=<username> ds_password=<password> profile_name=Basic summary
```

Related concepts

- [Big Data Intelligence with data marts](#)

Related reference

- [Big Data Intelligence APIs](#)

enable_datastream

Use the enable_datastream command to allow data streaming from cloud data sources.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/cloud_datasource
```

GuardAPI syntax

```
enable_datastream
```

Examples

This API takes no parameters.

```
grdapi enable_datastream
```

Related concepts

- [Cloud database service protection with datastreams](#)

Related reference

- [disable_datastream](#)
-

enable_disable_ip_restriction

This command allows you to specify one or more IP addresses for which you can restrict access by user type (SSH, GUI, or ALL).

When IP restriction is enabled, users can log into Guardium® only if they log in from an address that is on the *allowlist*.

Warning: Always assign one or more IP addresses to the allowlist from which you can access Guardium. If you restrict access to all IP addresses available to users, you will permanently lock all of your users (and yourself) out of Guardium.

This API is available in Guardium V11.4 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/ip_restriction
```

GuardAPI syntax

```
enable_disable_ip_restriction parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| allowlist | String | A comma-separated list of IP addresses for which you want to allow (or restrict) access. |
| enable | Boolean | Required. Specify whether logins are restricted to the IP addresses that are specified in the <i>allowlist</i> . Valid values: <ul style="list-style-type: none">• <i>false</i> (off) - Users can log in from any IP address.• <i>true</i> (on) - Users can log in only from specified addresses. Default = 1 (true) |
| type | String | Required. Specify whether to restrict access to the CLI (SSH), the GUI, or both (ALL) for the IP addresses in the <i>allowlist</i> . Valid values: <ul style="list-style-type: none">• <i>ALL</i> - Both SSH and GUI users.• <i>GUI</i> - Users who log into the Guardium GUI.• <i>SSH</i> - Users who log in to the CLI via SSH. Note: You can run this command multiple times to create allowlists for different login types. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• <i>all_managed</i>: execute on all managed units but not the central manager• <i>all</i>: execute on all managed units and the central manager• <i>group:<group name></i>: execute on all managed units identified by <i><group name></i>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Related reference

- [get_ip_restriction_config](#)
- [update_ip_restriction_allowlist](#)

Related information

- [Managing access by IP address](#)
-

enable_disable_monitoring_streams

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/monitor_datastream
```

GuardAPI syntax

```
enable_disable_monitoring_streams parameter=value
```

Amazon-specific parameters

| Parameter | Value type | Description |
|---------------------|------------|---|
| activate | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true): Start the data stream. Default = 0 (false) |
| cloudTitle | String | Required. The name of the cloud DB service account. For valid values, call enable_disable_monitoring_streams from the command line with --help=true.
For more information, see Define, modify, and delete AWS DB service accounts . |
| cluster_resource_id | String | Required. The cluster resource ID for the AWS RDS cluster associated with the stream. |
| collectorHostNames | String | Required. The names of your Guardium collectors, for example: collector01.yourcompany.com
For valid values, call enable_disable_monitoring_streams from the command line with --help=true. |
| consumerGroupName | String | Required. The consumer group name that you assign from the Guardium® Cloud DB Service Protection page. For more information, see Discover and configure AWS data streams . |
| db_DNS_endpoint | String | Required. The DB DNS endpoint. |
| port | String | Required. The DB DNS endpoint port. |
| region | String | Required. For valid values, call enable_disable_monitoring_streams from the command line with --help=true. |
| streamName | String | Required. The name of the stream from the RDS cluster configuration. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Azure-specific parameters

| Parameter | Value type | Description |
|-------------------------|------------|---|
| activate | Boolean | Activates data streaming. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true): Start the data stream Default = 0 (false) |
| cloudTitle | String | Required. The name of the cloud DB service account. For more information, see Define, modify, and delete Azure cloud database service accounts . |
| collectorHostNames | String | The names of your Guardium collectors, for example: collector01.yourcompany.com |
| consumerGroupName | String | The Azure consumer group name. |
| db_DNS_endpoint | String | Required. The DB DNS endpoint. |
| namespace | String | The Azure event hub namespace. |
| port | String | Required. The DB DNS endpoint port. |
| storageConnectionString | String | The Azure storage connection string name |
| streamName | String | Required. The event hub name. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related tasks

- [Define, modify, and delete AWS cloud DB service accounts](#)
- [Define, modify, and delete Azure cloud database service accounts](#)

enable_embed_eastern_font

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
enable_embed_eastern_font parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

enable_entitlement_optimization

This command enables the entitlement optimization feature on this Collector.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/enableEntitlementOptimization
```

GuardAPI syntax

```
enable_entitlement_optimization parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| | | |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • <code>all_managed</code>: execute on all managed units but not the central manager • <code>all</code>: execute on all managed units and the central manager • <code>group:<group name></code>: execute on all managed units identified by <code><group name></code> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapi enable_entitlement_optimization
```

Related concepts

- [Entitlement Optimization](#)

Related reference

- [Entitlement optimization APIs](#)

enable_fam_crawler

This command enables the FAM file crawler, which sends the file metadata and data from its discovery and classification processes to the Guardium system. The results are automatically added to quick search index files. Use the parameters to schedule quick search for file activity, and entitlement extractions.

Note: The Investigation Dashboard must also be enabled with the command `grdapi enable_quick_search schedule_interval=1`.

This API is available in Guardium V11.4, 11.5 and 12.0.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/enable_fam_crawler
```

GuardAPI syntax

```
enable_fam_crawler parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------------------|------------|--|
| activity_schedule_interval | String | Required. The frequency at which the database sends file activity audits to enterprise search. The recommended interval is 2 with <code>activity_schedule_units</code> set to MINUTE. |
| activity_schedule_units | String | Required. The unit for <code>activity_schedule_interval</code> . The recommended unit is MINUTE. Valid values: |
| | | <ul style="list-style-type: none"> • <code>HOUR</code> • <code>MINUTE</code> |
| entitlement_schedule_interval | String | Required. The frequency at which the database sends file entitlements and classifier results to the Guardium system. The recommended interval is 1 with the <code>entitlement_schedule_units</code> set to DAY. |
| entitlement_schedule_units | String | Required. The unit for <code>entitlement_schedule_interval</code> . The recommended unit is DAY. Valid values: |
| | | <ul style="list-style-type: none"> • <code>DAY</code> • <code>HOUR</code> • <code>MINUTE</code> |
| extraction_start | Date | Initial date/time from which data is extracted to the file quick search. The default is current time; the earliest time you can specify is 2 days ago. If the <code>entitlement_schedule_units</code> is set to HOUR, then it is rounded to an hour. If it is set to DAY, then it is rounded to a day. |
| schedule_start | Date | The default is current time. |

Examples

To enable the FAM crawler with the recommended values: file activity audit details are sent are sent every two minutes, and entitlement details are sent daily.

```
grdapi enable_fam_crawler activity_schedule_interval=2 activity_schedule_units=MINUTE entitlement_schedule_interval=1  
entitlement_schedule_units=DAY
```

Related concepts

- [FAM discovery and classification in Windows and UNIX-Linux file servers](#)
- [Using rules for file activity policies](#)

Related reference

- [add_action_to_fam_rule](#)
- [create_policy](#)
- [delete_policy](#)
- [create_fam_rule](#)
- [disable_fam_crawler](#)
- [get_fam_crawler_info](#)
- [list_policy_fam_rule](#)
- [policy_fam_rule_delete](#)

enable_fips_tls

The API disables TLS 1.3 on a standalone machine, a central manager, or a central manager and all associated managed units. Under some circumstances, for Guardium 12.0 or later, you must disable TLS 1.3 before you can enable FIPS 140 mode.

Before Guardium 12.0, Guardium supported TLS 1.0, 1.1, and 1.2. With the introduction of Guardium 12.0, Guardium supports TLS 1.2 and TLS 1.3. In all cases, Guardium supports the FIPS 140 protocol. However, in some cases, you must disable TLS 1.3 to enable FIPS 140 support.

Specifically, you might run into this issue if you upgrade your central manager to Guardium 12.x, but the managed units remain at pre-12.x releases. In this case, run `enable_fips_tls` on your central manager to disable TLS 1.3 and help ensure that Guardium supports the FIPS 140 protocol. For more information, see [Managing the TLS version](#).

Note: After you disable TLS 1.3, you need to enable FIPS mode and then reboot your server. There are two ways to enable FIPS mode.

- Run the [fipsmode](#) API. Guardium suggests that you set `restart = 1` to automatically restart your system.
- Run the [store_system_fipsmode](#) CLI command and then manually restart your system.

This API runs only on a central manager or standalone machine.

This API is available in Guardium v12.0 and later.

GuardAPI syntax

```
enable_fips_tls parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| all | Boolean | Required. Specify whether to disable TLS 1.3 on all associated managed units or only on the current unit. Valid values: <ul style="list-style-type: none">• 0 - Disable TLS 1.3 on the current unit only.• 1 - Disable TLS 1.3 on the current central manager (or standalone machine) and all associated managed units. Default = 0 (false) |
| force | Boolean | Valid values: <ul style="list-style-type: none">• 0 - Do not disable TLS 1.3 if the central manager and managed units are running different Guardium versions.• 1 - Disable TLS 1.3 even if there are differences between Guardium versions on the central manager and its associated managed units. Default = 0 (false) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Related tasks

- [Managing the TLS version](#)

Related reference

- [enable_all_tls](#)
- [enable_latest_tls](#)

enable_health_analyzer

This command enables the disk and database health analyzer.

By default, the analyzer sends alerts when the system predicts that the database size or files on a disk (/var) will reach 50% in the next 14 days. When enabled, it runs at a predefined schedule with a start time of 05:07:07. The schedule resets any time the health analyzer is enabled or re-enabled.

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/enableHealthAnalyzer
```

GuardAPI syntax

```
enable_health_analyzer parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • <code>all_managed</code>: execute on all managed units but not the central manager • <code>all</code>: execute on all managed units and the central manager • <code>group:<group name></code>: execute on all managed units identified by <code><group name></code> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Use this command to enable the disk and database health analyzer:

```
grdapicl enable_health_analyzer
```

Related reference

- [Health analyzer APIs](#)

enable_health_traffic_job

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/traffic_health
```

GuardAPI syntax

```
enable_health_traffic_job parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------|------------|--|
| enable | String | Required. Valid values: <ul style="list-style-type: none">• <i>true</i>• <i>false</i> |

enable_ip_to_host_aliases

This API enables the Guardium IP to hostname aliasing feature.

You can use

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/enable_ip_host_alias
```

GuardAPI syntax

```
enable_ip_to_host_aliases parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------------|------------|--|
| overrideExistingAliases | Boolean | <p>Required. If set to 1, override any existing found aliases.
Valid values:<ul style="list-style-type: none">• 0 (false)• 1 (true)</p> <p>Note: If your site has manually assigned alias names, you might not want to override them.</p> |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:<ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>.</p> <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related concepts

- [IP to Hostname Aliasing](#)

enable_latest_tls

Enable the most recent version of TLS (TLSv1.3) by disabling TLSv1.2 on either the current system or on all associated managed units.

Transport layer security (TLS) 1.3 provides a faster and more secure encryption protocol. Your Guardium central manager appliance must be at 12.0 or later. TLS 1.3 is automatically enabled with Guardium 12.x. You can choose to disable TLS 1.2 after your central manager, all associated managed units, S-TAPs, and the GIM client are at Guardium 12.x.

Note: Be very careful about forcing Guardium to disable TLS 1.2 if your configuration includes managed units that are not at Guardium 12.0. In addition, not all add-ons and features support TLS 1.3. For more information, see [Managing the TLS version](#).

Tip: This API takes a few minutes to run.

This API is available in Guardium v12.0 and later.

GuardAPI syntax

```
enable_latest_tls parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| all | Boolean | <p>Required. For a central manager, select whether to disable TLS 1.2 on all associated managed units. Valid values:</p> <ul style="list-style-type: none"> 0 (false) - Disable TLS 1.2 on this machine only. 1 (true) - Disable TLS1.2 on this machine and associated managed units. <p>Default = 0 (false)</p> |
| force | Boolean | <p>Specify whether to disable TLS 1.2 when appliance, GIM, or S-TAP versions are incompatible between the central manager and any managed units. Valid values:</p> <ul style="list-style-type: none"> 0 (false) - Do not disable TLS 1.2 if versions are incompatible. 1 (true) - Disable TLS 1.2 even if versions are incompatible. <p>Default = 0 (false)</p> |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> all_managed: execute on all managed units but not the central manager all: execute on all managed units and the central manager group:<group name>: execute on all managed units identified by <group name> host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related tasks

- [Managing the TLS version](#)

Related reference

- [enable_all_tls](#)
- [get_secured_protocols_info](#)

Related information

- [show_tls_enabled](#)

enable_monitoring_ranger_service

Use this command to enable a configured Ranger service (for Hadoop monitoring).

This command requires valid administrative authority on the Ambari server such as an admin or service administrator account. After running the command, the Ambari administrator must restart the affected Hadoop components so that the changes take effect.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/enable_monitoring_ranger_service
```

GuardAPI syntax

```
enable_monitoring_ranger_service parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|--|
| clusterName | String | Required. Ambari cluster name. |
| serviceName | String | Required. Name of the service. Valid values: <ul style="list-style-type: none"> hdfs hive hbase kafka solr storm |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GrdAPI example

To enable the HDFS service on Cluster4:

```
grdapiclusterName=Cluster4 serviceName=HDFS
```

Sample output:

```
ID=0
The Hadoop service configuration has been changed. Ask the Hadoop administrator to restart the Hadoop service to activate the changes.
HDFS Monitoring Disabled <server name>:5565
```

REST API Example

To enable the HIVE service:

```
curl -k --header "Authorization:Bearer <access token>" -i -H "Content-Type: application/json" -X PUT -d
'{clusterName="Cluster4", serviceName="HIVE"}' https://<guardium server>:8443/restAPI/enable_monitoring_ranger_service
```

Sample output:

```
[
  {
    "id": 3,
    "ambariConfigId": 1,
    "service": {
      "id": 1,
      "label": "HBase",
      "value": "HBASE"
    },
    "stapHost": {
      "id": 30,
      "name": "<Guardium server>",
      "value": "<Guardium server>",
      "port": "5534",
      "stapStatus": 2
    },
    "isMonitored": false,
    "port": "5534",
    "editMode": true
  },
  {
    "id": 1,
    "ambariConfigId": 1,
    "service": {
      "id": 2,
      "label": "HDFS",
      "value": "HDFS"
    },
    "stapHost": {
      "id": 30,
      "name": "<Guardium server>",
      "value": "<Guardium server>",
      "port": "5534",
      "stapStatus": 2
    },
    "isMonitored": false,
    "port": "5534",
    "editMode": true
  },
  {
    "id": 2,
    "ambariConfigId": 1,
    "service": {
      "id": 3,
      "label": "Hive",
      "value": "HIVE"
    },
    "stapHost": {
      "id": 30,
      "name": "<Guardium server>",
      "value": "<Guardium server>",
      "port": "5534",
```

```

        "stapStatus": 2
    },
    "isMonitored": true,
    "port": "5534",
    "editMode": true
}
]

```

Related concepts

- [Hadoop integration using Hortonworks and Apache Ranger](#)

Related reference

- [Hadoop monitoring APIs](#)
- [S-TAP Hadoop parameters](#)

enable_native_audit

This API enables DB Audit (native audit) on the specified datasource.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/enable_native_audit
```

GuardAPI syntax

```
enable_native_audit parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| datasource_name | String | Required. A cloud datasource defined in Guardium. |
| should_restart | Boolean | Valid values: <ul style="list-style-type: none"> • 0 (false) • 1 (true) Default = 0 (false) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Related tasks

- [Cloud database service protection with native audit](#)

Related reference

- [Native audit APIs](#)

enable_outliers_detection

Run this command to enable outliers detection.

The command affects the Guardium systems differently, depending on their setup.

Single CM environment

Enable outliers detection on a CM to enable outliers detection on all managed units, and on all units registered to the CM thereafter, by running the API command with no additional parameters. You can limit the scope to a list of units.

Enable outliers detection on a collector that extracts data to an aggregator. Outliers detection is enabled on the aggregator (if not already enabled) and the collector starts sending data to the aggregator.

Multi-CM environment

Enable outliers detection on a CM to enable outliers detection on all managed units, and on all units registered to the CM thereafter, by running the API command with no additional parameters. You can limit the scope to a list of units.

When you enable outliers on a collector that extracts data to an aggregator that is not in the same CM environment as the collector:

- The collector starts sending data to the aggregator
- The API responds with the name of the aggregator that needs to be enabled for outliers detection

When you enable outliers on an aggregator, outliers detection is enabled and collectors in the same CM environment start sending data. If the aggregator receives data from collectors in a different CM environment, the API responds with list of all collectors that need to be enabled for outliers detection.

To enable on individual aggregators or collectors, use the commands [enable_outliers_detection_cross_cm_agg](#) and [enable_outliers_detection_cross_cm_collector](#).

Single Collector

Run the command on a collector that does not extract data to an aggregator, to enable it locally.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/enable_outliers_detection
```

GuardAPI syntax

```
enable_outliers_detection parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------------|---|---|
| DAM_FAM | String | Specifies the type of outliers. Valid values: <ul style="list-style-type: none">• DAM• FAM Default = DAM. |
| extraction_start | date in format:
yyyy-mm-dd
hh:mm:ss | Delays the start of data extraction. When not specified, data extraction starts immediately. |
| managed_units_hostnames | String | Comma-separated list of specific managed units on which the command is executed. Optional when you run the API on the CM. |
| schedule_interval | String | Ignored. |
| schedule_start | Date | Ignored. |
| schedule_units | String | Ignored. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

Run this command on the CM to enable the outliers detection on all the units under the CM and on all units that will be registered to the CM thereafter:

```
grdapicl enable_outliers_detection
```

Run this command on the CM to enable the outliers detection on all the managed units of groupA:

```
grdapicl enable_outliers_detection group_descriptions=groupA
```

Run this command on the central manager of a cross-CM environment to enable outliers detection on the cross-CM aggregator:

```
grdapicl enable_outliers_detection
Machines found: [<server1>, <server2>]
Machines not found: []
Aggs: []
Cross CM aggs: [<server2>]
```

```
Cross CM Col: []
Standalone Coll: []
Enabling outlier detection on cross cm aggregator: <server2>. Please make sure that you have enabled outliers detection on the
following Cross-CM Collectors: [<server1>].
Analytic anomaly detection is enabled.
ok
```

Related tasks

- [Enabling and disabling outliers detection](#)

Related reference

- [Outliers detection APIs](#)

enable_outliers_detection_agg

Run this API on a central manager to enable outliers detection on the specified aggregator.

It also schedules the datamart that sends outlier data from the collectors (that are in this CM) to the aggregator. It does not enable outlier mining on the collectors.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/enableOutliersDetectionOnAgg
```

GuardAPI syntax

```
enable_outliers_detection_agg parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------------|---|---|
| aggregator_host_name | String | Required. Outliers detection is enabled on this aggregator. |
| DAM_FAM | String | Optional. Specifies the type of outliers. Valid values: <ul style="list-style-type: none">• DAM• FAM The default is DAM. |
| extraction_start | date in format:
yyyy-mm-dd
hh:mm:ss | Use if you want to delay the start of data extraction. When not specified, data extractions starts immediately. |
| schedule_interval | String | Ignored. |
| schedule_start | Date | Ignored. |
| schedule_units | String | Ignored. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To enable outliers detection on the aggregator `agg-sw`, run this command on the central manager of `agg-sw`:

```
grdapiclent enable_outliers_detection_agg aggregator_host_name=agg-sw
```

Related concepts

- [Outliers detection](#)

Related tasks

- [Enabling and disabling outliers detection](#)

Related reference

- [Outliers detection APIs](#)

enable_outliers_detection_cross_cm_agg

Run on a central manager to enable outliers detection on the collector(s) that send data to the specified aggregator(s). This is for use in a multi-central manager environment; the aggregator is in this central manager's environment but the collectors are managed by a different central manager.

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/enableOutliersDetectionCrossCMOnAgg
```

GuardAPI syntax

```
enable_outliers_detection_cross_cm_agg parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------------|---|---|
| aggregator_host_name | String | Required. |
| DAM_FAM | String | Optional. Specifies the type of outliers. Valid values: <ul style="list-style-type: none">• DAM• FAM The default is DAM. |
| extraction_start | date in format:
yyyy-mm-dd
hh:mm:ss | Optional. Delays the start of data extraction. When not specified, data extraction starts immediately. |
| schedule_start | Date | Ignored. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To disable outliers detection on the collectors that send data to the aggregator **agg-sw**, run this command on the CM of aggregator **agg-sw**:

```
disable_outliers_detection_agg aggregator_host_name=agg-sw
```

Related concepts

- [Outliers detection](#)

Related tasks

- [Enabling and disabling outliers detection](#)

Related reference

- [Outliers detection APIs](#)

enable_outliers_detection_cross_cm_collector

Run on a central manager to enable outliers on the specified collector(s) in this central manager's environment. This is for use in a multi-central manager environment; the collector is in this central manager's environment but the data is sent to an aggregator in another central manager's environment.

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/enableOutliersDetectionCrossCMOnCollector
```

GuardAPI syntax

```
enable_outliers_detection_cross_cm_collector parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------------|---|---|
| collector_host_names | String | The collectors whose analytic data is getting sent to an aggregator outside of its central environment. |
| DAM_FAM | String | The type of outlier data. Valid values: <ul style="list-style-type: none">• DAM• FAM |
| extraction_start | date in the format: yyyy-mm-dd hh:mm:ss | Use if you want to delay the start of data extraction. When not specified, data extraction starts immediately. |
| group_descs | String | |
| schedule_start | | Ignored. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To enable outliers detection on the collectors `coll1a`, `coll2a`, run this command on the central manager of the collectors:

```
enable_outliers_detection_cross_cm_collector collector_host_names=coll1a,coll2a
```

Related concepts

- [Outliers detection](#)

Related tasks

- [Enabling and disabling outliers detection](#)

Related reference

- [Outliers detection APIs](#)

enable_persistent_queue_universal_connector

Run this API to enable a Persistent Queue on Logstash inputs. Changes take effect only after reloading the configurations or restarting Logstash.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/enablePersistentQueue
```

GuardAPI syntax

```
enable_persistent_queue_universal_connector parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To enable on the current Guardium system:

```
grdapi enable_persistent_queue_universal_connector  
Guardium Universal Connector command has been executed.
```

Related concepts

- [Guardium universal connector](#)

Related reference

- [Guardium universal connector APIs](#)

enable_policy_analyzer

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/enable_policy_analyzer
```

GuardAPI syntax

```
enable_policy_analyzer parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

enable_quick_search

This command enables investigation dashboard functionality.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/enable_quick_search
```

GuardAPI syntax

```
enable_quick_search parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------|------------|---|
| all | Boolean | On a central manager only, use this parameter to enable quick search (investigation dashboard) on all of its managed units. Valid values: <ul style="list-style-type: none">• 0 (false): Do not enable on the central manager's managed units. (Enable on the central manager only.)• 1 (true): Enable on the central manager and all of its managed units. Default = 0 (false) |
| extraction_start | Date | The date by which to start the extraction of audit data for quick search. If this parameter is omitted, extraction starts immediately. |
| includeViolations | Boolean | Whether or not to include violations in the search indexes. Omitting violations can help reduce the size of search indexes. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| schedule_interval | String | Required. Together with the schedule_units parameter, this defines the interval for extracting audit data. For example, schedule_interval=2 schedule_units=MINUTE. |
| schedule_start | Date | Date on which to begin extracting data. |
| schedule_units | String | Required. Together with the schedule_interval parameter, this defines the interval for extracting audit data. For example, schedule_interval=2 schedule_units=MINUTE. Valid values: <ul style="list-style-type: none">• HOUR• MINUTE |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values:
Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To enable quick search on the current unit and all of its managed units:

```
disable_quick_search all=true
```

Related concepts

- [Investigation dashboard](#)

Related reference

- [Investigation dashboard APIs](#)

enable_riskspotter

Run this command on a central manager to enable RiskSpotter on all of the central manager's managed units, or on a stand-alone Guardium system.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/enable_riskspotter
```

GuardAPI syntax

```
enable_riskspotter parameter=value
```

This API takes no parameters.

Examples

Run this command on a central manager to enable RiskSpotter on all of its managed units:

```
grdapicl enable_riskspotter
```

Related concepts

- [Risk Spotter](#)

enable_special_attributes

This API enables non-admin users to view attributes for certain groups in Query-Report Builder.

Within Query-Report Builder, admin users can see all attributes while non-admin users can view only query attributes, except attributes that are designated as admin only (such as IDs). Use `enable_special_attributes` to allow non-admin users to view all of the attributes within a specified `attributesGroup`.

Note: When an attribute group is enabled, all of the attributes within that group are available.

Note: With the following exception, you do not need to restart the GUI for changes to take effect. If a report with the attributes of group F5 is added to My New Reports, a non-admin user does not have privileges to view the report until the GUI is restarted.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
enable_special_attributes parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| attributesGroup | String | Required. Valid values: <ul style="list-style-type: none">• <i>data set</i>• <i>ims</i>• <i>hive</i>• <i>apex</i>• <i>mapreduce</i>• <i>bi</i>• <i>ims/data set</i>• <i>f5</i>• <i>db2 i</i> |

Examples

The following example enables Hive attributes for all non-admin users:

```
grdapicl enable_special_attributes attributesGroup=hive
```

Sample output

```
> grdapicl enable_special_attributes attributesGroup=hive
Following Attributes have been Enabled: Hive Parsed SQL, Hive User, Hive Command, Hive Database,
Hive Table Name, Hive Error
ok
```

Related reference

- [disable_special_attributes](#)

enable_strong_cli_password

This command changes the password requirement from 8 to 15 characters for the CLI user.

After you change the password with this command, the CLI user must change their password again on first login.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/strong_cli_password
```

GuardAPI syntax

```
enable_strong_cli_password parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| confirmpassword | String | Required. Confirm the new password. |
| enable | Boolean | Required. Valid values: <ul style="list-style-type: none">• 0 (false): CLI password can be 8 characters.• 1 (true): CLI password must be 15 characters. |
| newpassword | String | Required. The new password for this user. |
| username | String | Required. The name of the user whose password you want to change. The name must be cli. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GuardAPI example

```
grdapic change_cli_password username=cli enable=1 newpassword="Strong!Pass1234!" confirmpassword="Strong!Pass1234!"
```

Related reference

- [change_cli_password](#)

enable_threat_detection_use_case

Use this command to specify which types of use cases are included in the threat detection analysis.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/enable_threat_detection_use_case
```

GuardAPI syntax

```
enable_threat_detection_use_case parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| | | |

| Parameter | Value type | Description |
|-----------------|------------|---|
| case_name | String | Required. For valid values, call enable_threat_detection_use_case from the command line with --help=true. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To add the grants use case to the threat detection analysis:

```
grdapi enable_threat_detection_use_case case_name=GRANTS
```

Related concepts

- [Threat detection analytics](#)

Related reference

- [Threat detection analytics APIs](#)

enable_threat_finder

Run this command on a CM or on a standalone unit to enable the threat finder functionality of the Active threat analytics.

Prerequisite: The investigation dashboard (quick search) is enabled.

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/enable_threat_finder
```

GuardAPI syntax

```
enable_threat_finder parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To enable threat finder on the standalone unit or on the CM environment:

```
grdapi enable_threat_finder
ID=0
ok
```

Related concepts

- [Advanced threat analytics](#)

Related reference

- [Threat detection analytics APIs](#)
-

encrypt_value

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/encrypt_value
```

GuardAPI syntax

```
encrypt_value parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| key | String | Required. |
| valueToEncrypt | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>; execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

execute_appUserTranslation

This command runs existing application user translations.

This command imports the user definitions for all of the configured applications from the Application User Translation Configuration page. Running this command is the same as selecting Run Once Now from Application User Translation Configuration.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/app_user_translation
```

GuardAPI syntax

```
execute_appUserTranslation parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi execute_appUserTranslation
```

Related concepts

- [Identify Users via Application User Translation](#)

execute_assessment

This command submits a security assessment to run.

This command is equivalent to running **Run Once Now** from the Security Assessment Finder. Submitting the job places the process on the Guardium® Job Queue, from where the system runs a single job at a time.

You can see the job Status and the Process Run ID from the Guardium Job Queue.

Note: A Security Assessment must exist before you call this API.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/execute_assessment
```

GuardAPI syntax

```
execute_assessment parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|---|
| assessmentDescription | String | Required. The name of the assessment to run. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi execute_assessment assessmentDesc="assessment1"
```

execute_auditProcess

This command runs a specified audit process.

This command is equivalent to running **Run Once Now** from the Audit Process Builder.

Note: Due to a CLI command heap size limitation, if the audit report returns large amounts of data, run the audit process from the GUI.
This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/audit_process
```

GuardAPI syntax

```
execute_auditProcess parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| auditProcess | String | Required. The name of the audit process to run. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapic execute_auditProcess auditProcess="Appliance Monitoring"
```

Related concepts

- [Building audit processes](#)

execute_autodetect_process

Use this command to run the tasks associated with the specified process. It cannot run if no tasks are defined for the process, or if the process is already running.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/execute_autodetect_process
```

GuardAPI syntax

```
execute_autodetect_process parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------|------------|--|
| process_name | String | Required. Name of the auto-discovery process |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To run the process myProcess:

```
grdapi execute_autodetect_process process_name=myProcess
```

Related concepts

- [Database auto-discovery](#)

Related reference

- [Auto-discovery APIs](#)

execute_cls_process

This command submits classification processes to the job queue.

Using `execute_cls_process` is equivalent to using Run Now from the Run discovery panel of the Discover Sensitive Data tool. It submits the process to the Guardium Job Queue which runs a single job at a time. Administrators can view the job status at Discover->Classification->Guardium Job Queue

Create a classification process before using this command.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/execute_cls_process
```

GuardAPI syntax

```
execute_cls_process parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| processName | String | Required. The name of the classification process to run. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi execute_cls_process processName=APITEST_Ccls_10001_1
```

execute_flatLogProcess

This command merges flat log information to the internal database.

Running this command is the same as running **Run Once Now** from the Flat Log Process page.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/execute_flatLogProcess
```

GuardAPI syntax

```
execute_flatLogProcess parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi execute_flatLogProcess
```

Related concepts

- [Flat Log Process](#)

execute_incidentGenProcess

This command generates incidents based on a defined query against the policy violations log.

This command is the equivalent of running Run Once Now from the Incident Generation Process page.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/execute_incident_gen_process
```

GuardAPI syntax

```
execute_incidentGenProcess parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| processId | Integer | Required. The process ID of the incident. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi execute_incidentGenProcess processId=20003
```

Related concepts

- [Incident Management](#)

execute_incidentGenProcess_byDetails

This command generates incidents based on a defined query (by query name) against the policy violations log.

Use the parameters to filter for specific incidents. This command is the equivalent of running Run Once Now from the Incident Generation Process page.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/execute_incident_gen_process_by_details
```

GuardAPI syntax

```
execute_incidentGenProcess_byDetails parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| categoryName | String | The incident category name. |
| queryName | String | Required. The name of the query. |
| severity | String | The incident severity. |
| threshold | Integer | Threshold. |
| user | String | The username. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi execute_incidentGenProcess_byDetails queryName="Policy Violation Count" user=admin severity=info
```

Related concepts

- [Incident Management](#)

execute_ldap_user_import

This command imports Guardium® user definitions from an LDAP server that is already configured in the LDAP User Import page (for accessmgr roles only).

The command is the equivalent of running Run Once Now from the LDAP User Import page.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/ldap_user
```

GuardAPI syntax

```
execute_ldap_user_import parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapic execute_ldap_user_import
```

Related concepts

- [Importing users from LDAP](#)

execute_populateGroupFromQuery

This command populates a group by running an existing query.

This command is the equivalent of running **Run Once Now** for a group that is populated by a query. If the group is not configured for import, an error message is returned.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/populate_group_from_query
```

GuardAPI syntax

```
execute_populateGroupFromQuery parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|----------------------------------|
| groupDesc | String | Required. The name of the group. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi execute_populateGroupFromQuery groupDesc="A test"
```

Related tasks

- [Populating groups](#)

export_certificate

Use this command to distribute a certificate from a central manager to some or all of its associated managed units.

This API is available in Guardium v11.3 and later.

Note: This command restarts the GUI.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/export_certificate
```

GuardAPI syntax

```
export_certificate parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|---|
| alias | String | Required. |
| check_mu | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true) • false • true <p>Default = 0 (false)</p> |
| file | String | |
| force | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true) <p>Default = 0 (false)</p> |
| host | String | <p>Required. The hostname, where host can be one of the following options:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • group:<group name>: execute on all managed units identified by <group name> • Hostname or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |
| restart_gui | Boolean | Default = 1 (true) |

Example

The following command exports the 'tomcat' certificate to managed units in the 'eastern-mus' managed unit group. Force is enabled to proceed to the next unit if one or more units failed to retrieve the certificate.

```
grdapi export_certificate alias=tomcat host=group:eastern-mus force=true
```

export_config

Use this command to propagate either Venafi or remote logging configurations from a central manager to some or all of its associated managed units.

This API is available in Guardium v11.3 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/export_config
```

GuardAPI syntax

```
export_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| force | Boolean | If set to 1 (true), propagate the requested configuration even if some managed units are offline. If set to 0 (false), all managed units must be online or the command fails with an error message.

Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true)• <i>false</i>• <i>true</i>
Default = 0 (false) |
| host | String | Required. The host name, where host can be one of the following: <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>group:<group name></code>: execute on all managed units identified by <group name>• Host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>host=10.0.1.123</code>.
IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |
| type | String | Required. Valid values: <ul style="list-style-type: none">• <code>venafi</code>• <code>remotelog</code> |

Example

The following command sends the remote logging configuration to managed units in the 'eastern-mus' managed unit group. Force is enabled to proceed to the next unit if one or more units fail to retrieve the configuration.

```
grdapi export_config type=remotelog host=group:eastern-mus force=true
```

The following command sends the Venafi configuration to managed units in the 'eastern-mus' managed unit group. Force is enabled to proceed to the next unit if one or more units fail to retrieve the configuration.

```
grdapi export_config type=venafi host=group:eastern-mus force=true
```

Related concepts

- [Remote loggers](#)

export_definition

Exported data is stored in /var/log/guard, for example /var/log/guard/exp_group_2023_05_03_18h28m15s.sql.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
export_definition parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| dataSet | String | Required. For valid values, call <code>export_definition</code> from the command line with <code>--help=true</code> . |
| exportToCSV | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| exportToXacml | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| itemName | String | Required. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

export_log_files

This command exports any compressed and rotated messages from /var/log to a specified target.

Messages (log files) must be in the format *messages-nnn* (for example *messages-1223232*).

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/export_logfiles
```

GuardAPI syntax

```
export_log_files parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| Port | String | |
| RemoteHost | String | Required. |
| RemotePassword | String | Required. |
| RemotePath | String | Required. |
| RemoteUser | String | Required. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GrdAPI examples

To export log files to a remote host:

```
grdapi export_log_files RemoteHost=9.70.165.194 RemotePassword="password"  
RemotePath="/var/log/" RemoteUser="root"
```

To export log files on a specific port:

```
grdapi export_log_files RemoteHost=9.70.165.194 RemotePassword="password"  
RemotePath="/var/log/" RemoteUser="root" Port=22
```

REST API example

```
curl -k -i --header "Authorization: Bearer <token>" -i -H "Content-Type: application/json" -X POST -d '  
{\"RemoteHost\":\"9.70.165.194\", \"RemotePassword\":\"password\", \"RemotePath\":\"/var/log\", \"RemoteUser\":\"root\" }'  
' https://9.42.32.28:8443/restAPI/export_logfiles
```

export_transfer_key

Use this command to export the SSH transfer keys for the central manager and optionally for the managed units in a deployment, for SCP and SFTP file transfers for archive, data export, and system backup.

This API is available in Guardium v11.3 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/export_transfer_key
```

GuardAPI syntax

```
export_transfer_key parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| host | String | Required. The remote host to which you send the key pair. |
| password | String | Required. The user for the remote host. |
| user | String | Required. The password for the remote host user. |

api_target_host String

Specifies the target hosts where the API executes. Valid values:

- all_managed: execute on all managed units but not the central manager
- all: execute on all managed units and the central manager
- group:<group name>: execute on all managed units identified by <group name>
- host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, `api_target_host=10.0.1.123`.
- host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, `api_target_host=10.0.1.123`.

IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.

Examples

On the central manager, copy the unique public-transfer-key of each managed unit to the remote host, by entering:

```
grdapi export_transfer_key host="remote_host_1" user="user1" password="password" api_target_host=all
```

On a managed unit, copy the specific, unique, public-transfer-key of the managed unit to the remote host, by entering:

```
grdapi export_transfer_key host="remote_host_1" user="user1" password="password"
```

Related tasks

- [Enabling SSH key pairs for data archive, data export, data mart](#)

f5_add_apps_config

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
f5_add_apps_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| appsIP | String | Required. |
| bigIP | String | Required. |

f5_add_data_params

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
f5_add_data_params parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| maxData | Integer | |
| minData | Integer | |
| paramName | String | Required. |

f5_delete_apps_config

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
f5_delete_apps_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| appsIP | String | Required. |
| bigIP | String | Required. |

f5_delete_data_params

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
f5_delete_data_params parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| paramName | String | Required. |

f5_list_apps_config

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
f5_list_apps_config parameter=value
```

This API takes no parameters.

f5_list_data_params

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
f5_list_data_params parameter=value
```

This API takes no parameters.

f5_update_data_params

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
f5_update_data_params parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| maxData | Integer | |
| minData | Integer | |
| paramName | String | Required. |

fipsmode

Enable or disable Federal Information Processing Standard (FIPS) cryptographic standards.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/fipsmode_status
```

GuardAPI syntax

```
fipsmode parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| enable | Boolean | Required. Enable or disable FIPS mode. Valid values: <ul style="list-style-type: none">• 0 (false) - Disable FIPS mode.• 1 (true) - Enable FIPS mode. |
| restart | Boolean | After you enable or disable FIPS mode, you must restart your system. Specify whether to automatically restart. Valid values: <ul style="list-style-type: none">• 0 (false) - Do not automatically restart the system after you enable or disable FIPS mode.• 1 (true) - Automatically restart after you enable or disable FIPS mode. Default = 1 (true) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group: <group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

GrdAPI example:

```
sys-vm01.rtp.raleigh.ibm.com> grdapic fipsmode enable=1 restart=0
ID=0
=====
Please reboot the machine to complete the process.
=====
```

REST API example:

```
curl -k -i --header "Authorization: Bearer <token>" -i -H "Content-Type: application/json" -X POST -d \
{enable:1, restart:1}
' https://9.32.132.87:8443/restAPI/fipsmode_status
```

flatten_hierarchical_groups

This command flattens all groups that exist in the group builder.

When flattening hierarchical groups, all members of all child groups become direct members of the parent group.

This API is available in Guardium V9.5 and later.

This API takes no parameters.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/flatten_hierarchical_groups
```

GuardAPI syntax

```
flatten_hierarchical_groups
```

Examples

```
grdapic flatten_hierarchical_groups
```

generate_ssl_key_universal_connector

Run this API to configure an SSL connection, instead of the default TCP/UDP connection. This API prints the private key and public certificate to CLI. You need to copy it, and configure it on Filebeat (uncomment the lines as described in the configuration file) on your MongoDB server.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/generateSSLKeyUniversalConnector
```

GuardAPI syntax

```
generate_ssl_key_universal_connector parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| expiration_days | Integer | Default = 100 |
| hostname | String | Hostname of the Guardium machine that generated the API, or wildcard (see default value). Default value: *.guard.swg.usma.ibm.com |
| overwrite | Boolean | Overwrite the existing key and certificate, if they exist. Valid values: <ul style="list-style-type: none">• 0: no• 1: yes Default = 0 (no) |

Examples

To generate the SSL key:

```
grdapi generate_ssl_key_universal_connector hostname=<collector name>
Guardium Universal Connector command has been executed.
```

Related concepts

- [Guardium universal connector](#)

Related reference

- [Guardium universal connector APIs](#)

generate_transfer_key

Use this command to generate individual sets of SSH key pairs for the central manager, and optionally for each managed unit in a deployment, used for SCP and SFTP file transfers of archive, data export, and system backup.

This API is available in Guardium v11.3 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/generate_ssh_keys
```

GuardAPI syntax

```
generate_transfer_key parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Enter this command on the central manager to generate a key pair for the central manager:

```
grdapi generate_transfer_key
```

Enter this command on the central manager to generate a key pair for the central manager and all managed units:

```
grdapi generate_transfer_key api_target_host=all
```

Related tasks

- [Enabling SSH key pairs for data archive, data export, data mart](#)

getFieldsTitles

The search REST API returns the codes for column names, rather than the column (or field) names themselves. getFieldsTitles maps those codes to the actual column names.

The numbers that are returned are in response to search RESTAPI results.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available only as a REST service with the **GET** method. Call this API as follows:

GET https://[Guardium hostname or IP address]:8443/restAPI/fieldsTitles

This API takes no parameters.

Examples

Use this API to return a map of all column codes and their names in a search query. For example:

```
curl -k --header "Authorization: Bearer 3499f352-aa98-4046-89d8-aba3d8c7d0fc"  
"https://xxx.xxx.xxx:8443/restAPI/getFieldsTitles"
```

Returns the following information:

```
{  
    "Message": { "19": "Number of Instances",  
                "35": "Execute Privileged Groups",  
                "36": "Execute Privileged Users",  
                "18": "Anomaly Score",  
                "33": "Write Privileged Groups",  
                "15": "Violation",  
                "34": "Write Privileged Users",  
                "16": "Severity",  
                "39": "Modification Time",  
                "13": "Details",  
                "14": "Error",  
                .  
                .  
                .  
                "9": "Time",  
                "8": "Date"}},  
    "ID": 0  
}
```

Related reference

- [search](#)

getOAuthTokenExpirationTime

This API displays the expiration time of the REST API token.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
getOAuthTokenExpirationTime parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related reference

- [setOAuthTokenExpirationTime](#)

get_all_modifiable_guard_params

This generic command returns the list of parameters that can be modified with the API `modify_guard_param`.

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/get_all_modifiable_guard_params
```

GuardAPI syntax

```
get_all_modifiable_guard_params parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| paramdesclike | String | |
| paramlike | String | |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group: <group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Example

```
grdapi get_all_modifiable_guard_params
```

get_assessment_result

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/assessment_result
```

GuardAPI syntax

```
get_assessment_result parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|--|
| assessmentDescription | String | |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group: <group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

get_cluster_members

This API returns all of the members of a specified S-TAP cluster.

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/get_cluster_members
```

GuardAPI syntax

```
get_cluster_members parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|-------------|
| clusterName | String | Required. |

get_clusters

This API returns a list of all of the S-TAP clusters on this system.

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/get_clusters
```

GuardAPI syntax

```
get_clusters parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

get_datamart_info

This command returns details on the datamart, for example, the report and query on which the datamart is based, creation date, results are extracted to file or initial start, time granularity, and so on.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
get_datamart_info parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------|------------|--|
| datamart_name | String | Required. |
| isExtended | Boolean | <p>Valid values:</p> <ul style="list-style-type: none">• 0 (false)• 1 (true) <p>Default = 0 (false)</p> |

Examples

To output info on data mart Export:RD1:

```
grdapi get_datamart_info datamart_name="Export:RD1"
=====
Data Mart Name: Export:RD1
=====
Description:
Based on Query: RD1
Extract result to: File
Initial Start: 2020-06-24 06:06:00
Creation Date: 2020-06-24 07:13:09
Time Granularity: 20 MINUTE
Active: true
-----
Customized Date Format:
File Name: EXP_RD1
Lines per File: 0
File Header: "UTC Offset","% CPU Mysql","% CPU Sniffer","% Mem Mysql"
Include File Header: true
-----
Copy File Info
-----
Host Name: <hostname>
Failover Host Name: <failover hostname>
Port # :
User Name: root
Directory: /var/tmp/
Password: *****
Transfer Method: SCP
Bundle Name:
Bundle Main Datamart: false
Send COMPLETE File: true
-----
Last Extraction Info
-----
State:1
-----
Timestamp: 2020-06-29 09:09:50
Next Period: 2020-06-29 09:06:00
Last Extracted ID: 0
-----
Extraction Log
-----
Timestamp: 2020-06-29 09:10:48
Extract Status: OK
Start Time: 2020-06-29 09:09:49
End Time: 2020-06-29 09:09:50
Period Start: 2020-06-29 08:46:00
Period End: 2020-06-29 09:06:00
Records Extracted: 20
Details: SCP to: <hostname to which it was exported>, User: root, Path: /var/tmp/, File: 2542225914053566522_<hostname data was
exported from>.EXP_RD1_20200629124600.gz
Last for Period: true
File Name: /opt/IBM/Guardium/data/dump/DATAMART/EXP_RD1_20200629124600.csv
Bundle Name:
File Transfer Status: Done
ok
```

Related concepts

- [Data mart](#)

Related reference

- [Data mart APIs](#)

get_datasource_custom_properties

This command lists all available custom property names and associated values.

This API is available in Guardium V11.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/datasource_custom_prop
```

GuardAPI syntax

```
get_datasource_custom_properties parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Example

The following command lists all datasource custom properties that are configured in your Guardium® system.

```
grdapi get_datasource_custom_properties
```

Related concepts

- [Datasource APIs](#)

get_debug_level

This command returns the debug level for IMS output.

This API is available in Guardium V10.1.4 and later.

GuardAPI syntax

```
get_debug_level parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related reference

- [set_debug_level](#)

get_definitions_data_sets

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available only as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/get_definitions_data_sets
```

GuardAPI syntax

`get_definitions_data_sets`

This API takes no parameters.

`get_definitions_items`

Run this command to return a list of the possible items to export for a given data set type or category.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available only as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/get_definitions_items
```

GuardAPI syntax

```
get_definitions_items parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| dataSet | String | A defined data set. For valid values, call <code>get_definitions_items</code> from the command line with <code>--help=true</code> . |

`get_distributed_report_target_info`

Run this API to see the list of Guardium systems defined as targets for distributed reports.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
get_distributed_report_target_info
```

This API takes no parameters.

Examples

To return the list of defined targets for distributed reports:

```
grdapic get_distributed_report_target_info
```

Related concepts

- [Distributed report builder](#)

Related reference

- [Reports and report generation APIs](#)

`get_entitlement_optimization_info`

Displays the entitlement optimization configuration for all data sources on this Collector.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/getEntitlementOptimizationInfo
```

GuardAPI syntax

```
get_entitlement_optimization_info
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Example

```
grdapi get_entitlement_optimization_info
```

Sample output:

```
Entitlement Optimization is enabled
=====
Datasource: DB16
=====
isEnabled: true
userScope:
objectScope:
extractActivity: true
extractEntitlement: true
generateRoleClusters: true
generateNews: true
generateRecommendations: true
filterTempObjects: true
filterIgnoreVerbs: true
=====
Datasource: SSQLSERVER
=====
isEnabled: true
userScope:
objectScope:
extractActivity: true
extractEntitlement: true
generateRoleClusters: true
generateNews: true
generateRecommendations: true
filterTempObjects: true
filterIgnoreVerbs: true
```

Related concepts

- [Entitlement optimization](#)

Related reference

- [Entitlement optimization APIs](#)

get_expiration_date_for_restored_day

This command returns the expiration date for data restored from the specified date.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/expiration_date_for_restored_day
```

GuardAPI syntax

```
get_expiration_date_for_restored_day parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|--|
| restoredDay | String | Required. Identifies the day whose data was restored. The format is one of: real day <code>yyyy-mm-dd hh:mi:ss</code> ; or relative day such as <code>NOW -10 day</code> . |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To return the expiration date for restored data, dated 10 days ago:

```
grdapi get_expiration_date_for_restored_day restoredDay=NOW -10 day
```

Related tasks

- [Managing stored data](#)

Related reference

- [Archive, export, import, purge, and restore APIs](#)

get_extraction_profile_info

Lists one or more GBDI (Big Data) profiles and whether they are active, and optionally the datamarts and schedules for each profile.

This API is available in Guardium V10.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/extractionProfile
```

GuardAPI syntax

```
get_extraction_profile_info parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| profile_name | String | If specified, it is used as search filter, returning all profile names containing the specified string. |
| verbose | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • 0 (false): lists the profile name and indicates if a profile is active. • 1 (true): lists the datamarts and schedules for each profile. <p>Default = 0 (false)</p> |
| verbosity_flags | String | |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

View details of the profile `sql_all`.

```
get_extraction_profile_info profile_name=sql_all verbose=1
```

Related concepts

- [Big Data Intelligence with data marts](#)

Related reference

- [Data mart APIs](#)

get_fam_crawler_info

Shows the status of the FAM crawler. If it is enabled, the response also shows the settings for the entitlement extraction and the quick search file activity schedule.

This API is available in Guardium V11.4, 11.5 and 12.0.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/get_fam_crawler_info
```

GuardAPI syntax

```
get_fam_crawler_info
```

Examples

```
grdapic get_fam_crawler_info
```

Two typical responses, for FAM crawler disabled, and FAM crawler enabled:

FAM Crawler (server side) is disabled.

FAM Crawler (server side) is enabled. Entitlement(1 DAY) Activity(2 MINUTE)

Related concepts

- [FAM discovery and classification in Windows and UNIX-Linux file servers](#)
- [Using rules for file activity policies](#)

Related reference

- [enable_fam_crawler](#)
- [disable_fam_crawler](#)
- [add_action_to_fam_rule](#)
- [create_fam_rule](#)
- [list_policy_fam_rule](#)
- [policy_fam_rule_delete](#)

get_flatLogProcessType

This command displays the processType of the current flat log file.

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/flatLogProcessType
```

GuardAPI syntax

```
get_flatLogProcessType parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi get_flatLogProcessType
```

Sample output:

```
ID=1
FLAT_LOG_PROCESS_TYPE:1 - Process
```

Related concepts

- [Flat Log Process](#)

get_guard_param

This generic command returns the current value of parameters that can be modified with the API `modify_guard_param`.

This API is available in Guardium V10.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/get_guard_param
```

GuardAPI syntax

```
get_guard_param parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| paramdesc | String | |
| paramName | String | |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapi get_guard_param
```

```
grdapi get_guard_param paramName=classifier_running_timeout
```

get.hadoop_cluster_status

This API returns the status of a Hadoop cluster on a specified host. This command only checks to see that the S-TAP® has been set up as a remote logger for Ranger.

This command does not validate that auditing is turned on at Ranger or that traffic is actually flowing. You need to run reports or look in the investigation dashboard on the appliance to see if traffic is flowing to the appliance.

This API is available in Guardium V10.1.4 and later.

The REST API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/get_hadoop_cluster_status
```

GuardAPI syntax

```
get_hadoop_cluster_status parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|--|
| clusterName | String | Required. The name of the cluster. |
| password | String | Required. Password for the cluster. |
| serverHostName | String | Required. Ambari host name. |
| serverPort | Integer | Ambari port. |
| sslEnabled | Boolean | Valid values: <ul style="list-style-type: none">• 0: false• 1: true Default = 0 |
| userName | String | Required. Admin ID for Ambari. |

API example

```
grdapi get_hadoop_cluster_status serverHostName=<server name> serverPort=8080 userName=admin password=admin clusterName=c5HDFS
Monitoring EnabledHBASE
Monitoring EnabledHIVE
Monitoring EnabledKAFKA
Monitoring Enabled
```

Related concepts

- [Linux-UNIX: Hadoop integration using Hortonworks and Apache Ranger](#)

Related reference

- [Hadoop monitoring APIs](#)

get_health_traffic_status

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/traffic_health
```

GuardAPI syntax

```
get_health_traffic_status parameter=value
```

Parameters

get_inapplicable_test_result_status

This API is available in Guardium v11.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/inapplicable_test_result_status
```

GuardAPI syntax

```
get_inapplicable_test_result_status parameter=value
```

get_insights_agent_config

List all of the Guardium® Insights task manager parameters.

To update the Guardium Insights task manager parameters, use the [update_insights_agent_config](#) GuardAPI.

Important: Some parameters display for informational purposes only and cannot be changed.

This API is available in Guardium v11.3 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/insights_agent_config
```

GuardAPI syntax

```
get_insights_agent_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| paramName | String | Displays the value of the specified parameter. |

Related reference

- [update_insights_agent_config](#)

get_ip_restriction_config

This command displays whether IP restriction is enabled or disabled.

This API is available in Guardium V11.4 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/ip_restriction
```

GuardAPI syntax

```
get_ip_restriction_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
> grdapi get_ip_restriction_config
ID=0
IP allowlist for GUI: Enabled
IP allowlist for SSH: Disabled
```

Related reference

- [enable_disable_ip_restriction](#)
- [update_ip_restriction_allowlist](#)

Related information

- [Managing access by IP address](#)

get_ip_to_alias_overwrites

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/ip_to_alias_overwrites
```

GuardAPI syntax

```
get_ip_to_alias_overwrites parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

get_ip_to_alias_selected

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/ip_to_alias_selected
```

GuardAPI syntax

```
get_ip_to_alias_selected parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

get_istap_config

Run this command to view the configuration parameters, including the current filtering options, for an S-TAP® on an IBM i server.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/istap_config
```

GuardAPI syntax

```
get_istap_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|---|
| datasourceName | String | Required. IP or name of the IBM i server. |

Examples

Run this command to see the S-TAP configuration on the IBM i server with the IP 11.11.11.11:

```
grdapic get_istap_config datasourceName=11.11.11.11
```

Related concepts

- [DB2 for IBM i S-TAP](#)

Related reference

- [S-TAP for IBM i APIs](#)

get_istap_status

Run this command to check whether the IBM i audit server is running. The output includes additional information (such as the number of messages on the queue, the size of the message queue, and so on) that can be useful for troubleshooting and performance tuning.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/istap_status
```

GuardAPI syntax

```
get_istap_status parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|---|
| datasourceName | String | Required. IP or name of the IBM i server. |

Examples

Run this to see the status of the IBM i server with the IP 11.11.11.11:

```
grdapi get_istap_status datasourceName=11.11.11.11
```

Related concepts

- [DB2 for IBM i S-TAP](#)

Related reference

- [S-TAP for IBM i APIs](#)

get_job_process_concurrency_limit

This command shows the job process concurrency limit.

This API is available in Guardium V10.6 and later.

GuardAPI syntax

```
get_job_process_concurrency_limit parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> all_managed: execute on all managed units but not the central manager all: execute on all managed units and the central manager group:<group name>: execute on all managed units identified by <group name> host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapi set_job_process_concurrency_limit
```

get_kafka_clusters

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/kafka_cluster
```

GuardAPI syntax

```
get_kafka_clusters parameter=value
```

get_load_balancer_load_map

This API returns the current load balancer map.

You can filter the map by managed unit, S-TAP®, or IP address.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
get_load_balancer_load_map parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| muHost | String | The managed unit host name. |
| stapHost | String | Host name of the server where the S-TAP is installed. You can enter a full or partial name. Guardium finds partial values only if the S-TAP is stored as corresponding value. |
| stapIP | String | The S-TAP IP address. You can enter the full or a partial address. Guardium finds partial values only if the S-TAP is stored as corresponding value. |

Related tasks

- [Viewing the enterprise load balancing load map](#)

get_load_balancer_params

This API returns the current load balancer configuration parameters.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
get_load_balancer_params
```

This API takes no parameters.

Related reference

- [Enterprise load balancing configuration parameters](#)

get_mfa_configuration

This command displays the current multi-factor authentication settings for the GUI, CLI, and SSH.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/configure_mfa
```

GuardAPI syntax

```
get_mfa_configuration parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related concepts

- [Portal configuration](#)

get_native_audit_collectors

This API returns the name of the collector, in your environment, that is receiving data from the specified host, port, and service name.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/nau_collectors_list
```

GuardAPI syntax

```
get_native_audit_collectors parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| host | String | Required. The hostname or the IP address of the server that is hosting the database that you are monitoring. |
| port | Integer | Required. |
| service_name | String | Required. For a Db2 data source, enter the database name. For other data sources, enter the service name. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related tasks

- [Cloud database service protection with native audit](#)

Related reference

- [Native audit APIs](#)

get_native_audit_configurations

This API returns details about the specified host, port, and service name. Information includes cloud environment ID, cloud environment, provider, datasource ID, instance name, database engine, service name, host, port, Guardium security group, objects limit, objects, and collector.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/nau_configurations
```

GuardAPI syntax

```
get_native_audit_configurations parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| host | String | Required. The hostname or the IP address of the server that is hosting the database that you are monitoring. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| port | Integer | Required. |
| service_name | String | Required. For a Db2 data source, enter the database name. For other data sources, enter the service name. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related tasks

- [Cloud database service protection with native audit](#)

Related reference

- [Native audit APIs](#)

get_native_audit_objects

This API returns all objects that are found by the classification process on the specified host, port, and service name.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/nau_objects_list
```

GuardAPI syntax

```
get_native_audit_objects parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| host | String | Required. The hostname or the IP address of the server that is hosting the database that you are monitoring. |
| port | Integer | Required. |
| service_name | String | Required. For a Db2 data source, enter the database name. For other data sources, enter the service name. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related tasks

- [Cloud database service protection with native audit](#)

Related reference

- [Native audit APIs](#)

get_outliers_detection_info

Use this command to output: whether outliers is enabled, for DAM or FAM, the user mode, when the learning started, and the factory and current settings for outliers parameters.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
get_outliers_detection_info parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

All parameters are described in [set_outliers_detection_parameter](#).

To get the outliers detection parameter settings for the Guardium system on which you are logged in, enter:

```
grdapi get_outliers_detection_info
```

Sample output:

```
Analytic anomaly detection is enabled. (DAM)
Learning since: 2020-01-12 12:03:18
```

```
Factory settings
-----
alertsPerDay=24.0
budgetTrainingDays=14
cleanupKeepDays=90
clusteringScheduleIntervals=24
debugMode=false
demoMode=0
intervalAlertsThreshold=0.99
maxMessageAlertsSampleSizePerAlertType=5
maxMessageAlertsTopScores=20
messageAlertsThreshold=0.9
minDaysForAlerts=7
minNumIntervalsForFirstClustering=168
minNumIntervalsForIntervalScorers=20
minNumIntervalsForMessageScorers=20
nanny.duration.analysis=60m
nanny.duration.clean=30m
nanny.duration.maintenance=2h
nanny.duration.reconfig=5m
numOfAnalyzeThreads=-1
privUsersGroup=Admin Users
runCaseAnalysis=true
sensitiveFileGroup=Sensitive Files
sensitiveObjectGroup=Sensitive Objects
```

```
Current
-----
alertsPerDay=100
budgetTrainingDays=14
cleanupKeepDays=90
clusteringScheduleIntervals=1
debugMode=false
demoMode=1
intervalAlertsThreshold=0.5
maxMessageAlertsSampleSizePerAlertType=5
maxMessageAlertsTopScores=20
messageAlertsThreshold=0.9
minDaysForAlerts=0
minNumIntervalsForFirstClustering=1
minNumIntervalsForIntervalScorers=2
minNumIntervalsForMessageScorers=2
nanny.duration.analysis=60m
nanny.duration.clean=30m
```

```

nanny.duration.maintenance=2h
nanny.duration.reconfig=5m
numOfAnalyzeThreads=-1
privUsersGroup=Admin Users
runCaseAnalysis=true
sensitiveFileGroup=Sensitive Files
sensitiveObjectGroup=Sensitive Objects
ok

```

Related tasks

- [Enabling and disabling outliers detection](#)

Related reference

- [Outliers detection APIs](#)
- [set_outliers_detection_parameter](#)

get_policy_analyzer_status

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/get_policy_analyzer_status
```

GuardAPI syntax

```
get_policy_analyzer_status parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • <code>all_managed</code>: execute on all managed units but not the central manager • <code>all</code>: execute on all managed units and the central manager • <code>group:<group name></code>: execute on all managed units identified by <code><group name></code> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

get_purge_batch_size

This API returns the current setting for the purge batch size on one or more Guardium® systems. The batch size is the incrementation in which purges are processed.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
get_purge_batch_size parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To view the current purge batch size:

```
grdapi get_purge_batch_size
```

Sample output:

```
ID=0
Purge Batch Size = 300000
ok
```

Related tasks

- [Managing stored data](#)

Related reference

- [Archive, export, import, purge, and restore APIs](#)

get_quick_search_info

This command returns whether quick search is enabled.

This GuardAPI is available in Guardium V9.5 and later.

The REST API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/quick_search
```

GuardAPI syntax

```
get_quick_search_info parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To determine whether quick search is enabled:

```
grdapi get_quick_search_info
Quick Search is enabled.
```

Related concepts

- [Investigation dashboard](#)

Related reference

- [Investigation dashboard APIs](#)

get_ranger_config

This command returns the Ambari administrator ID, Ambari server name, and Ambari port for the specified Ambari cluster.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/get_ranger_config
```

GuardAPI syntax

```
get_ranger_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| clusterName | String | Required. Ambari cluster name. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GrdAPI example

To view the configuration of the cluster named Cluster4:

```
grdapi get_ranger_config clusterName=Cluster4
```

System response:

```
admin@<server>:<port> Cluster4 SSL enabled: true
```

REST API example

To view the configuration of the cluster named Cluster4:

```
curl -k -i --header "Authorization:Bearer <access token>" https://<Guardium server name>:8443/restAPI/get_ranger_config?
clusterName=Cluster4
```

Sample output:

```
[{"id": 1, "clusterName": "Cluster4", "serverHost": "<server>", "serverPort": 8080, "userName": "admin", "lastRefresh": "2016-10-03 18:06:31", "status": []}]
```

Related concepts

- [Hadoop integration using Hortonworks and Apache Ranger](#)

Related reference

- [Hadoop monitoring APIs](#)
- [S-TAP Hadoop parameters](#)

get_ranger_hdfs_config

Use this command to output the details of the Hadoop integration with Ranger HDFS that sends data to the specified S-TAP.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/get_ranger_hdfs_config
```

GuardAPI syntax

```
get_ranger_hdfs_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| stapHostName | String | Required. Host name or IP of the S-TAP® that receives the Ranger audit messages from the Ranger. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To view details of the Hadoop integration that sends data to the S-TAP nn.nn.nn.nn:

```
grdapi get_ranger_hdfs_config stapHostName=nn.nn.nn.nn  
ID=0  
rangerHDFSauditDirs :  
/ranger/audit/hive/hiveServer2,/ranger/audit/kafka/kafka,/ranger/audit/hbase/hbaseMaster,/ranger/audit/hbase/hbaseRegional,/ranger/audit/atlas/atlas,/ranger/audit/hdfs/hdfs,/ranger/audit/impala/impala,/ranger/audit/knox/knox,/ranger/audit/solr/solr  
rangerHdfsKeytab : /usr/local/guardium/guard_stap/hdfs.keytab  
rangerHdfsLibLocation : /opt/cloudera/parcels/CDH-7.1.1-1.cdh7.1.1.p0.2879197/lib64  
rangerHdfsNameNode : null  
rangerHdfsPollMs : 100  
rangerHdfsPort : 8020  
useKerberos : true  
ldLibrary : /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.252.b09-2.el7_8.x86_64/jre/lib/amd64/server  
principal : hdfs/cdp711-11.fyre.ibm.com@DBANET4.ROOT  
  
ok
```

Related concepts

- [Hadoop integration using Ranger HDFS for Hortonworks and Cloudera 7](#)

Related reference

- [Hadoop monitoring APIs](#)
- [S-TAP Hadoop parameters](#)

get_ranger_services_status

Use this command to view status of the ranger services, optionally on a specified cluster. It does not necessarily indicate that traffic is flowing.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/get_ranger_services_status
```

GuardAPI syntax

```
get_ranger_services_status parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| clusterName | String | Use this parameter to restrict the output to the status of this cluster only. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GrdAPI example

To view the status on the cluster named Cluster4:

```
grdapic get_ranger_services_status clusterName=Cluster4
```

Sample output:

```
admin@hw-cl4-05:8080 Cluster4
```

REST API example

To view the services that are set up to be monitored:

```
curl -k -i --header "Authorization:Bearer <access token>" https://<Guardium server name>:8443/restAPI/get_ranger_services_status?clusterName=Cluster4
```

Sample output, showing services that are not currently monitored ("id": 0 and "ambariConfigId": -1):

```
[  
  {  
    "id": 0,  
    "ambariConfigId": -1,  
    "service": {  
      "id": 2,  
      "label": "HDFS",  
      "value": "HDFS"  
    },  
    "isMonitored": false,  
    "editMode": false  
  },  
  {  
    "id": 0,  
    "ambariConfigId": -1,  
    "service": {  
      "id": 3,  
      "label": "Hive",  
      "value": "HIVE"  
    },  
    "isMonitored": false,  
    "editMode": false  
  },  
  {  
    "id": 0,  
    "ambariConfigId": -1,  
    "service": {  
      "id": 1,  
      "label": "HBase",  
      "value": "HBASE"  
    },  
    "isMonitored": false,
```

```

    "editMode": false
},
{
  "id": 0,
  "ambariConfigId": -1,
  "service": {
    "id": 5,
    "label": "Storm",
    "value": "STORM"
  },
  "isMonitored": false,
  "editMode": false
},
{
  "id": 0,
  "ambariConfigId": -1,
  "service": {
    "id": 4,
    "label": "Kafka",
    "value": "KAFKA"
  },
  "isMonitored": false,
  "editMode": false
}
]

```

Related concepts

- [Hadoop integration using Hortonworks and Apache Ranger](#)

Related reference

- [Hadoop monitoring APIs](#)
- [S-TAP Hadoop parameters](#)

get_registered_units

REST API syntax

12.1 and later This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/get_registered_units
```

GuardAPI syntax

```
get_registered_units parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| secretKey | String | Required. Default value = 0 |
| unitIp | String | Required. Default value = 0 |
| unitPort | String | Required. Default value = 0 |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> <code>all_managed</code>: execute on all managed units but not the central manager <code>all</code>: execute on all managed units and the central manager <code>group:<group name></code>: execute on all managed units identified by <code><group name></code> host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

get_secured_protocols_info

This API returns the version of TLS that is enabled or disabled on both a central manager and its managed units.

For Guardium 12.0 and later use this API to see the Guardium and TLS versions for the central manager, all managed units, the GIM client, and any S-TAPs As you upgrade managed units, S-TAPs and so on to Guardium 12.0, you can use the [enable_latest_tls](#) API to enable TLS 1.3.

This API is available in Guardium V10.1.4 and later.

GuardAPI syntax

```
get_secured_protocols_info parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| fullscan | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

get_solr_cluster_info

Use this command, on a central manager only, to output details on the Solr cluster: the registered managed units and their status.

The output is written to /var/IBM/Guardium /log/solr_cluster_info.txt. (The output can be very large if there are many MUs).

This API is available in Guardium V10.6 and later.

GuardAPI syntax

```
get_solr_cluster_info parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

```
grdapic get_solr_cluster_info
```

Sample response:

```
Please see the following file for results: /var/IBM/Guardium/log/solr_cluster_info.txt
```

Related reference

- [Solr APIs](#)

get_solr_errors

This command outputs exceptions/warnings from the solr.

This API is available in Guardium V10.1.4 and later.

GuardAPI syntax

```
get_solr_errors parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| logToFile | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

```
grdapic get_solr_errors
```

Related reference

- [Solr APIs](#)

get_solr_status

This command returns the status of solr installation on the specified Guardium® system(s).

This command can return a few outputs (which can be translated on ApplicationResources.properties). If solr is not enabled:

- If solr is not enabled: Solr is not enabled on this machine
- If solr is enabled but not running: Solr is not running
- If solr is enabled and running: Solr is running

This API is available in Guardium V10.6 and later.

GuardAPI syntax

```
get_solr_status parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------|------------|---|
| get_error_details | Boolean | If this parameter is set to true and solr is not running because of some exception, this exception is also written to console. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapi get_solr_status get_error_details=true
```

Related reference

- [Solr APIs](#)

get_solr_status_extended

This command returns the status of solr installation on the specified Guardium® systems.

This API is similar to [get_solr_status](#), but get_solr_status_extended makes additional checks to determine if solr is running.

This API is available in Guardium v12.0 and later.

GuardAPI syntax

```
get_solr_status_extended parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------|------------|---|
| get_error_details | Boolean | <p>If this parameter is set to true and solr is not running because of some exception, this exception is also written to console. Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true) <p>Default = 0 (false)</p> |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

get_streams

This API returns configuration information for the AWS data streams or Azure event hubs for the specified cloud DB service account (cloudTitle).

For this API, the following rules apply for status information:

- REST API: When available, returns the status, along with configuration information, for the stream or event hub.
- GuardAPI:
 - On a central manager: Returns configuration information. In addition, if the stream is assigned to a collector, then the API also returns the status of the stream for that collector.
 - On stand-alone or managed units: Configuration information displays, but status is not available.

Status information is available in the UI at Discover > Database Discovery > Cloud DB Service Protection. Select a Cloud database service account to see status and other information.

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/datasream
```

GuardAPI syntax

```
get_streams parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| cloudTitle | String | Required. The name of the cloud DB service account. For valid values, call <code>get_streams</code> from the command line with <code>--help=true</code> . For more information, see Define, modify, and delete AWS cloud DB service accounts . |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related concepts

- [Manage AWS data streams](#)
- [Manage Azure event hubs](#)

get_test_result_detail_string_setting

This command displays the tables into which the detailed test findings for a vulnerability assessment are written.

This API is available in Guardium V11.4 and later.

This API takes no parameters.

For backward compatibility, Vulnerability Assessment (VA) continues to store all detailed test results in one record in addition to creating a separate record for each detailed finding. The API command `get_test_result_detail_string_setting` displays the entities into which the detailed test findings are written.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/detail_string_setting
```

GuardAPI syntax

```
get_test_result_detail_string_setting parameter=value
```

Example

Example 1:

```
grdapi get_test_result_detail_string_setting
ID=0
Test details are written to the TEST_RESULT_DETAIL and TEST_RESULT tables.
ok
```

Example 2:

```
grdapi get_test_result_detail_string_setting
ID=0
Test details are written only to the TEST_RESULT_DETAIL table.
ok
```

Related reference

- [Assessment APIs](#)

get_threat_detection_use_case_info

Run this command to see which types of use cases are included in the threat detection analysis.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/threat_detection_use_case_info
```

GuardAPI syntax

```
get_threat_detection_use_case_info parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To see which use case types are included in the threat detection analysis:

```
grdapi get_threat_detection_use_case_info
Use case: INSIDER_THREAT - disabled
Use case: GRANTS - enabled
Use case: STP - enabled
Use case: SQL_INJECTION - enabled
```

Related concepts

- [Threat detection analytics](#)

Related reference

- [Threat detection analytics APIs](#)

get_unit_data

This command returns details about the current appliance, including the host name and IP address, unit type, Guardium version, and information about the most recently installed patch.

This API is available in Guardium v11.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/unit_data
```

GuardAPI syntax

```
get_unit_data parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

get_unit_pinger

This API queries the internal UnitPinger thread.

Note: This command must be called with `api_target_host=127.0.0.1` parameter.
This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
get_unit_pinger parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|-------------|
| name | String | |
| api_target_host | String | 127.0.0.1 |

Examples

```
grdapi get_unit_pinger api_target_host=127.0.0.1
```

Related reference

- [restart_unit_pinger](#)

get_universal_connector_allowed_domains

Run this API to output a list of cloud-based database domains that are authorized for communication with the local or specified Guardium system.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/getUcAllowedDomains
```

GuardAPI syntax

```
get_universal_connector_allowed_domains parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To list the allowed domains on the local system:

```
grdapi get_universal_connector_allowed_domains
ID=0
amazonaws.com
ok
```

Related reference

- [Guardium universal connector APIs](#)

get_universal_connector_status

Returns the status of the Guardium universal connector, on the local or the specified collectors.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/getUniversalConnectorStatus
```

GuardAPI syntax

```
get_universal_connector_status parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

This output indicates a fully running Guardium universal connector:

```
grdapi get_universal_connector_status
ID=0
Guardium Universal Connector is running.
ok
```

This output indicates a disabled universal connector:

```
grdapi get_universal_connector_status
ID=0
Guardium Universal Connector is disabled.
ok
```

Related concepts

- [Guardium universal connector](#)

get_va_summary_key

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/get_va_summary_key
```

GuardAPI syntax

```
get_va_summary_key
```

This API has no parameters.

get_wkc_config

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/wkc
```

GuardAPI syntax

```
get_wkc_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| units | String | |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

get_ztap_logging_config

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/ztap_logging_config
```

GuardAPI syntax

```
get_ztap_logging_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

gim_assign_bundle_or_module_to_client_by_version

Assigns a bundle a module to a client, based on the module version.

This API is similar to `gim_assign_latest_bundle_or_module_to_client`, except that you must specify the exact version of the module or bundle to assign.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/gim_client_assign
```

GuardAPI syntax

```
gim_assign_bundle_or_module_to_client_by_version parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------|------------|------------------------------|
| clientIP | String | Required. Client IP address. |
| module | String | Required. |
| moduleVersion | String | Required. |

Examples

```
grdapic Gim_assign_bundle_or_module_to_client_by_version clientIP=192.168.1.100 module=BUNDLE-STAP moduleVersion="8.0_r1234_1"
```

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

gim_assign_latest_bundle_or_module_to_client

Use the `gim_assign_latest_bundle_or_module_to_client` API to assign the latest (that is, the highest version) available bundle or module to a specified client.

This API is similar to `gim_assign_bundle_or_module_to_client_by_version`. However `gim_assign_latest_bundle_or_module_to_client` always assigns the most recent version of the bundle or module to the client.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/gim_assign_latest_bundle
```

GuardAPI syntax

```
gim_assign_latest_bundle_or_module_to_client parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------|------------|-------------|
| clientIP | String | Required. |
| module | String | Required. |

Examples

```
grdapi gim_assign_latest_bundle_or_module_to_client clientIP=192.168.1.100 module=BUNDLE_STAP
```

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

gim_cancel_install

Cancel the installation of a bundle or module for a specified client.

Use this API to cancel installing a module or bundle that is not being installed by a client (that is, STATE=IP or IP-PR).

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/gim_cancel_install
```

GuardAPI syntax

```
gim_cancel_install parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| clientIP | String | Required. |
| module | String | Required. |

Examples

Cancel the installation of the BUNDLE-STAP module.

```
grdapi gim_cancel_install clientIP=192.168.1.100 module=BUNDLE-STAP
```

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

gim_cancel_uninstall

Use this API to cancel the scheduled uninstall of a specified bundle or module for a client.

You can cancel an uninstall only if the module or bundle is not being uninstalled (that is STATE=IP or IP-PR).

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/gim_cancel_uninstall
```

GuardAPI syntax

```
gim_cancel_uninstall parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| clientIP | String | Required. |
| module | String | Required. |

Examples

```
grdapi gim_cancel_uninstall clientIP=192.168.1.100 module=BUNDLE-STAP
```

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

gim_get_available_modules

List the modules or bundles available to install on a specified server.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/gim_available_modules
```

GuardAPI syntax

```
gim_get_available_modules parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| clientIP | String | Required. |

Examples

```
grdapi gim_get_available_modules clientIP=192.168.1.100
```

Related concepts

- [Guardium Installation Manager](#)

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

gim_get_client_last_event

List the latest operation executed for a specified client.

This API shows the last event that occurred during the latest installation attempt. For example, if there were errors during the latest installation of S-TAP, you can run `gim_get_last_event` to show the errors. However, if you manually fix the installation problem directly on the database server, this command still shows the same original error message (even though S-TAP is now running). Do not use `gim_get_last_event` to evaluate S-TAP status after you make manual fixes on the database server.
This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/gim_client_last_event
```

GuardAPI syntax

```
gim_get_client_last_event parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| clientIP | String | Required. |

Examples

Use the clientIP to specify where to look for the latest events. For example:

```
grdapi gim_get_client_last_event clientIP=192.168.1.100  
grdapi gim_get_client_last_event clientIP=winx64
```

Related concepts

- [Guardium Installation Manager](#)

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

gim_get_global_param

Return the value of a GIM global parameter.

This API is available in Guardium V10.1.4 and later.

GuardAPI syntax

```
gim_get_global_param parameter=value
```

Parameters

| Parameter | Value type | Description |
|---|------------|--|
| paramName | String | Required. Name of the parameter to set, listed in the following table. |
| Parameter name | Value type | Description |
| auto_install_on_db_server_os_upgrade | Boolean | If enabled, automatically upgrade modules when the client operating system vendor version changes. Valid values: <ul style="list-style-type: none">• 0: Disabled• 1: Enabled Default = 0
For more information, see Linux®-UNIX: Managing GIM clients when upgrading your database server operating system , and Managing S-TAP when upgrading your database operating system . |
| dynamic_alive_enabled | Boolean | Controls the dynamic alive feature. Valid values: <ul style="list-style-type: none">• 0: Disabled• 1: Enabled Default = 0
For more information, see GIM dynamic updating . |
| enable_secure_unauthenticated_communication | Boolean | If enabled, allow unauthenticated GIM communication over a secure port: communication between the GIM client and server are encrypted with SSL on port 8444, but the communication is handled without using certificates for peer authentication. Valid values: <ul style="list-style-type: none">• 0: Disabled• 1: Enabled Default = 0
The enable_secure_unauthenticated_communication allows distributing new GIM client certificates when it is time to replace certificates. |
| gim_auto_certificate_distribution | Boolean | Controls automatic distribution of certificates to GIM clients. Valid values: <ul style="list-style-type: none">• 0: disabled• 1: enabled Default = 0
For more information, see Create and manage GIM certificates . |
| gim_file_upload_token | string | Define the GIM file upload exchange token. |
| gim_listener_default_port | string | Define the GIM listener default port.
Default = 88445

For more information, see Gim server allocation . |
| gim_listener_default_shared_secret | string | Define the GIM listener encrypted shared secret.
For more information, see Gim server allocation . |
| gim_quick_start_enable | Boolean | Controls the GIM quick start feature. Valid values: <ul style="list-style-type: none">• 0: disabled• 1: enabled Default = 0 |

Examples

Return the value of the gim_listener_default_port parameter.

```
grdapi gim_get_global_param paramName=gim_listener_default_portID=0
8445
ok
```

Related concepts

- [Guardium Installation Manager](#)

Related reference

- [gim_set_global_param](#)
- [Guardium Installation Manager \(GIM\) APIs](#)

gim_get_modules_running_status

List the modules or bundles currently running on a specific server.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
gim_get_modules_running_status parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| clientIP | String | Required. The client IP address |
| process | String | The process name |
| status | String | Valid values are: <ul style="list-style-type: none">• ON• OFF |

Examples

```
grdapi gim_get_modules_running_status clientIP=192.168.1.100 process= status=
```

Related concepts

- [Guardium Installation Manager](#)

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

gim_list_bundles

Use the gim_list_bundles API to list all of the available bundles for a client. A bundle is a group of modules that can be installed on a client.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/gim_bundle
```

GuardAPI syntax

```
gim_list_bundles
```

Examples

This API takes no parameters:

```
grdapi gim_list_bundles
```

Related concepts

- [Guardium Installation Manager](#)

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

gim_list_client_modules

Lists all the modules that are assigned to a specific client along with their state.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/gim_list_client_modules
```

GuardAPI syntax

```
gim_list_client_modules parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| clientIP | String | Required. |

Examples

```
grdapi gim_list_client_modules clientIP=192.168.2.210
```

Related concepts

- [Guardium Installation Manager](#)

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

gim_list_client_params

Lists all of the (module) parameters that are assigned to a specific GIM client.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/gim_client_params
```

GuardAPI syntax

```
gim_list_client_params parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|------------------------------|
| clientIP | String | Required. Client IP address. |

Examples

```
grdapi gim_list_client_params clientIP=192.168.12.210
```

Related concepts

- [Guardium Installation Manager](#)

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)
-

gim_list_mandatory_params

Lists all of the required parameters for the specified version of a module.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
gim_list_mandatory_params parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| module | String | Required. |
| version | String | Required. |

Examples

Both the module name and module version number are required. For example:

```
grdapic Gim_list_mandatory_params module=name version=number
```

Related concepts

- [Guardium Installation Manager](#)
-

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)
-

gim_list_registered_clients

Lists all the registered clients for Guardium Installation Manager (GIM).

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/gim_registered_clients
```

GuardAPI syntax

```
gim_list_registered_clients
```

Examples

List all of the registered GIM clients for your site.

```
grdapic Gim_list_registered_clients
```

Related concepts

- [Guardium Installation Manager](#)
-

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)
-

gim_list_unused_bundles

Returns a list of unused (not installed on any database server) bundles and individual Windows modules that can be uploaded (for example, Windows CAS or Windows FAM).

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/list_unused_bundles
```

GuardAPI syntax

```
gim_list_unused_bundles parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| includeLatest | Boolean | Required. If set to 1, the returned list includes the latest unused bundle. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

The following example returns a list of unused bundles, including the most recent:

```
grdapi gim_list_unused_bundles includeLatest=1
```

Related concepts

- [Guardium Installation Manager](#)

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

gim_load_package

Loads all of the modules within a specified filename.

Note: This command loads one or more files that reside on the local file system. Therefore, the procedure (cmd='fileserver') of loading a file to the CM/Guardium appliance must precede this command.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/gim_package
```

GuardAPI syntax

```
gim_load_package parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------|------------|-------------|
| filename | String | Required. |

Examples

The following example finds all files with the file type 'gim'. Use the * (asterisk) as a wildcard to find files.

```
grdapic Gim_load_package filename=*.gim
```

Related concepts

- [Guardium Installation Manager](#)

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

gim_remote_activation

Connects the collector's IP address to a server mode GIM agent or group of GIM agents.

This API is available in Guardium V10.1.4 and later.

GuardAPI syntax

```
gim_remote_activation parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------------|------------|---|
| connectToCollector | String | The appliance to which you want the GIM listener or client to connect to after it is activated. |
| sharedSecret | String | The shared secret that was configured during installation. |
| targetGroup | String | The group name of all the database servers that the collector connects to.
You can specify either targetGroup or targetHost, but not both. |
| targetHost | String | The database server on which the GIM listener is running.
You can specify either targetGroup or targetHost. |
| targetPort | Integer | The port server mode of the GIM agent. |

Examples

```
grdapic Gim_remote_activation targetGroup=<someGroup> sharedSecret=<password> targetPort=8445
```

Related concepts

- [Guardium Installation Manager](#)

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

gim_remove_bundle

Delete a bundle from both the database and the file system.

You can use the wildcard character (*) to delete all unassigned bundles.

The gim_remove_bundle API removes a specified bundle from both /var/log/guard/gim_packages, and, if the Guardium® system is a central manager, from /var/gim_dist_packages.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/gim_remove_bundle
```

GuardAPI syntax

```
gim_remove_bundle parameter=value
```

| Parameter | Value type | Description |
|-------------------|------------|--|
| bundlePackageName | String | Required. The value must be unique and refer to an existing bundle that is not assigned to any client. Specify an asterisk (*) to delete all unassigned bundles. |

Examples

To specify a bundle to delete:

```
grdapi gim_remove_bundle bundlePackageName= hadriansBundle
```

To delete all unassigned bundles:

```
grdapi gim_remove_bundle bundlePackageName=*
```

Sample output:

```
Failed removing bundle (Can't delete module BUNDLE-GIM 11.5.0_r105891_1 as part of bundle guard-BUNDLE-GIM-10.5.0_r105891_v10_5_1-r1)
BUNDLE_PACKAGE removed:guard-GIM-guardium_11.5_r100500139_1-Windows-Server-Windows-x86_x64.exe.signed
BUNDLE_PACKAGE removed:guard-BUNDLE-STAP-11.5.0_r102753_trunk_1-suse-11-linux-x86_64.tar.gz.signed
BUNDLE_PACKAGE removed:guard-BUNDLE-STAP-11.5.0_r103055_v11_5_1-rhel-6-linux-x86_64.tar.gz.signed
ID=0
```

Related concepts

- [Guardium Installation Manager](#)

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)
- [gim_list_unused_bundles](#)

gim_reset_client

Refresh connection to the specified client by disassociating and re-associating the GIM module.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
gim_reset_client parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| clientIP | String | Required. |

Examples

```
grdapi gim_reset_client clientIP=192.168.1.100
```

Related concepts

- [Guardium Installation Manager](#)

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

gim_schedule_install

Schedules installation for all the modules or bundles that are assigned to a client, but are not yet installed.

Schedules the installation of modules or bundles that are, for example, in a PENDING state. If you specify the module parameter , only the requested module is scheduled.

Note: Schedule a past date to run the job immediately.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/gim_schedule_install
```

GuardAPI syntax

```
gim_schedule_install parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| clientIP | String | Required. |
| date | String | Required. The installation date in the format now or yyyy-MM-dd HH:mm |
| module | String | If module is not specified, all of the modules for the specified clientIP are scheduled for installation. |

Examples

Schedule an installation for one or more modules.

```
grdapi gim_schedule_install clientIP=192.168.1.100 module=BUNDLE-STAP date="2019-07-02 14:50"
```

```
grdapi gim_schedule_install clientIP=192.168.1.100 date="2019-07-02 14:50"
```

Related concepts

- [Guardium Installation Manager](#)

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

gim_schedule_uninstall

Schedule an uninstall of the module or bundles that are assigned to a client but are not yet uninstalled (that is, in PENDING state).

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/gim_schedule_uninstall
```

GuardAPI syntax

```
gim_schedule_uninstall parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| clientIP | String | Required. |
| date | String | Required. The installation date in the format now or yyyy-MM-dd HH:mm |
| module | String | If module is not specified, all of the modules for the specified clientIP are scheduled for the uninstall. |

Examples

The following example schedules an uninstall for the BUNDLE-STAP module:

```
grdapi gim_schedule_uninstall clientIP=192.168.1.100 module=BUNDLE-STAP date="2019-07-02 14:50"
```

The following example schedules an uninstall for all of the client's modules:

```
grdapi gim_schedule_uninstall clientIP=192.168.1.100 date="2019-07-02 14:50"
```

Related concepts

- [Guardium Installation Manager](#)

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

gim_set_diagnostics

Set diagnostics collection within GIM.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
gim_set_diagnostics parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| clientIP | String | Required. |

Examples

```
grdapi gim_set_diagnostics clientIP=192.168.1.100
```

Related concepts

- [Guardium Installation Manager](#)

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

gim_set_global_param

Use this API to set global parameters for GIM clients.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
gim_set_global_param parameter=value
```

Parameters

| Parameter | Value type | Description |
|---|------------|---|
| paramName | String | Required. Name of the parameter to set, listed in the following table. |
| paramValue | String | Required. The value for the paramName. |
| Parameter name | Value type | Description |
| auto_install_on_db_server_os_upgrade | Boolean | If enabled, automatically upgrade modules when the client operating system vendor version changes. Valid values: <ul style="list-style-type: none"> • 0: Disabled • 1: Enabled Default = 0
For more information, see Linux®-UNIX: Managing GIM clients when upgrading your database server operating system , and Managing S-TAP when upgrading your database operating system . |
| dynamic_alive_enabled | Boolean | Controls the dynamic alive feature. Valid values: <ul style="list-style-type: none"> • 0: Disabled • 1: Enabled Default = 0
For more information, see GIM dynamic updating . |
| enable_secure_unauthenticated_communication | Boolean | If enabled, allow unauthenticated GIM communication over a secure port: communication between the GIM client and server are encrypted with SSL on port 8444, but the communication is handled without using certificates for peer authentication. Valid values: <ul style="list-style-type: none"> • 0: Disabled • 1: Enabled Default = 0
The enable_secure_unauthenticated_communication allows distributing new GIM client certificates when it is time to replace certificates. |

| Parameter name | Value type | Description |
|------------------------------------|------------|--|
| gim_auto_certificate_distribution | Boolean | Controls automatic distribution of certificates to GIM clients. Valid values: <ul style="list-style-type: none">• 0: disabled• 1: enabled Default = 0
For more information, see Create and manage GIM certificates . |
| gim_file_upload_token | string | Define the GIM file upload exchange token. |
| gim_listener_default_port | string | Define the GIM listener default port.
Default = 88445

For more information, see Gim server allocation . |
| gim_listener_default_shared_secret | string | Define the GIM listener encrypted shared secret.
For more information, see Gim server allocation . |
| gim_quick_start_enabled | Boolean | Controls the GIM quick start feature. Valid values: <ul style="list-style-type: none">• 0: disabled• 1: enabled Default = 0 |

Examples

Set the value of gim_listener_default_port.

```
grdapi gim_set_global_param paramName=gim_listener_default_port paramValue=8445
```

Related concepts

- [Guardium Installation Manager](#)

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

gim_unassign_client_module

Unassign a module from a client.

Unlike gim_remove_module, this command undoes the connection between a module and a specific client on the central manager, but does not uninstall or remove the module on the actual database server.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/gim_unassign_client_module
```

GuardAPI syntax

```
gim_unassign_client_module parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| clientIP | String | Required. |
| module | String | |

Examples

To unassign the STAP module from the client:

```
grdapi gim_unassign_client_module clientIP=192.168.1.100 module=STAP
```

Related concepts

- [Guardium Installation Manager](#)

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

gim_uninstall_module

Uninstalls a module or bundle for a specific client.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/gim_uninstall_module
```

GuardAPI syntax

```
gim_uninstall_module parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| clientIP | String | Required. |
| date | String | The date and time to uninstall in the format now or yyyy-MM-dd HH:mm |
| module | String | Required. |

Examples

Uninstall the BUNDLE-STAP module immediately:

```
grdapi gim_uninstall_module clientIP=192.168.1.100 module=BUNDLE-STAP
```

Related concepts

- [Guardium Installation Manager](#)

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

gim_update_client_params

Updates a single module parameters in a specific client.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/gim_client_params
```

GuardAPI syntax

```
gim_update_client_params parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|--|
| clientIP | String | Required. IP address of target client. |
| paramName | String | Required. |
| paramValue | String | |

Examples

```
grdapi gim_update_client_params clientIP=192.168.1.100 paramName=STAP_TAP_IP paramValue=192.168.1.100
```

Related concepts

- [Guardium Installation Manager](#)

Related reference

- [Guardium Installation Manager \(GIM\) APIs](#)

grant_role_to_object_by_Name

This command assigns a role to a specified object by names.

Guardium checks the dependencies before it adds the role. For example, before Guardium adds a role to a Classification process, the role must be assigned to all components that are contained by that process (that is, the classification policy and any datasources that it references).

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/grant_role_to_object_by_Name
```

GuardAPI syntax

```
grant_role_to_object_by_Name parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| objectName | String | Required. The name of the object (such as a query or report) to which to assign the role. When objectName is set to <code>ALL</code> , the role that is specified is assigned to all objects. |
| objectType | String | Required. The type of object to which to assign the role. For valid values, call <code>grant_role_to_object_by_Name</code> from the command line with <code>--help=true</code> . |
| role | String | Required. The name of the role to assign. Specify any existing role. Specify <code>all_roles</code> to allow access by all roles. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • <code>all_managed</code>: execute on all managed units but not the central manager • <code>all</code>: execute on all managed units and the central manager • <code>group:<group name></code>: execute on all managed units identified by <code><group name></code> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI examples

```
grdapapi grant_role_to_object_by_Name objectType=Datasource objectName= "swanSybase" role=admin  
grdapapi grant_role_to_object_by_Name objectType="SecurityAssessment" objectName="ALL" role="user"
```

When the object Name is set to `ALL`, the role of `user` is assigned to all objects of type `SecurityAssessment`.

Related concepts

- [Understanding Roles](#)

grant_role_to_object_by_id

This command assigns a role to a specified object by IDs.

Guardium checks the dependencies before it adds the role. For example, before Guardium adds a role to a Classification process, the role must be assigned to all components that are contained by that process (that is, the classification policy and any datasources that it references).

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/grant_role_to_object_by_id
```

GuardAPI syntax

```
grant_role_to_object_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| objectId | Integer | Required. The ID of the object to assign the role to. |
| objectTypeId | Integer | Required. The type of object. For valid values, call grant_role_to_object_by_id from the command line with --help=true. |
| roleId | Integer | Required. The ID of the role to assign to the object. Specify any existing role ID or specify -1 to allow access by all roles. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi grant_role_to_object_by_id objectTypeId=13 objectId=2 roleId=3
```

Related concepts

- [Understanding Roles](#)

health_info

This API is available in Guardium v11.3 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/health_info
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| requestorId | String | |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

import_definitions

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available only as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/import_definitions
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| file | File | |

insights_registration

This API allows you to register Guardium® Data Protection to Guardium Insights that allows you to use Guardium Insights data with Guardium Data Protection features such as health and data mart reports.

This API is available in Guardium v11.3 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/insights_registration
```

GuardAPI syntax

```
insights_registration parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|--|
| insights_apikey_token | String | Required. An API token that is generated from Guardium Insights to allow external sources to execute RESTAPI calls on Guardium Insights. The token includes the encrypted Guardium Insights tenant ID. |
| insights_ca_cert_cn | String | The Insights certificate common name that is generated when the certificate is created. During the registration process, you can specify the certificate common name to verify the CN field as part of the standard certificate exchange authentication. |
| insights_url | String | Required. The Guardium Insights URL. |

Related reference

- [insights_unregistration](#)
- [update_insights_registration_config](#)

insights_unregistration

This API removes the registration information for Guardium® Insights from Guardium Data Protection.

This API is available in Guardium v11.3 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/insights_registration
```

GuardAPI syntax

```
insights_unregistration
```

Related reference

- [insights_registration](#)
- [update_insights_registration_config](#)

kill_running_process

This API stops a long-running process.

Use the [list_running_processes](#) API to find the process ID of the process you want to stop.

For more information about long running processes, see [list_running_processes](#).

You can view or change the timeout duration from either the Running Query Timeout page in the UI or by using the [show_maximum_query_duration](#) and [store_maximum_query_duration](#) APIs.

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/kill_running_process
```

GuardAPI syntax

```
kill_running_process parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| processID | Long | Required. The ID of the process to stop. |

Examples

The following examples both stop process 74 from running.

```
grdapi kill_running_process processID=74

curl \
-k --header "Authorization:Bearer 395fea0f-4cbf-487d-90ef-d2241c5843c6" \
-i -H "Content-Type:application/json" \
-X POST "https://test.usma.ibm.com:8443/restAPI/kill_running_process/?processID=74"
```

Related reference

- [list_running_processes](#)
- [show_maximum_query_duration](#)
- [store_maximum_query_duration](#)

list_adhoc_policy_analyzer

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/list_adhoc_policy_analyzer
```

GuardAPI syntax

```
list_adhoc_policy_analyzer parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

list_aliases

Use the `list_aliases` command to show some or all of the current aliases for a specified object.

Use list_aliases to show any aliases that meet the specified criteria.
Note: Some special rules apply to the syntax for the API parameters:

- The groupTypeDescLike parameter always evaluates as Like. For example, if you pass in the value `IP`, the API evaluates the value as `%IP%`.
- The ampersand (&) character is required between each parameter and must have an escape, Enter it as `&&`.
- For the values of dbValueLike and aliasValueLike, use the Like operator (%) to return partial matches. However, % is a special character that is passed as `%25` (25 is the ASCII representation of %).

Therefore, the parameters in a curl command must appear as shown in the following example:

```
...aliasListing/?groupTypeDescLike=IP&&dbValueLike=%25&&aliasValueLike=%25
```

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/alias
```

GuardAPI syntax

```
list_aliases parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------|------------|--|
| aliasValueLike | String | All or part of an alias name. |
| dbValueLike | String | All or part of a database name. |
| groupTypeDescLike | String | Required. All or part of the Group Type description (such as ClientIP or Service Name) for an alias. |

Examples

The following example returns all of the aliases from IP objects (such as client or server IP) where the alias ends with the number one.

```
test.usma.ibm.com> grdapi list_aliases groupTypeDescLike="IP" aliasValueLike="%1" dbValueLike="%"
```

This command provides the following output:

```
ID=0
ERR=0
Group Type: Client IP DB Value: 1.2.3.4 Alias Value: A1
Group Type: Client IP DB Value: 2.3.3.6 Alias Value: B1
Group Type: Server IP DB Value: 5.6.7.8 Alias Value: C1
ok
```

The following example returns all of the aliases from IP objects (such as client or server IP) where the alias contains the letter "C".

```
[tester@oc3843647344 ~]$ curl \
-k --header "Authorization:Bearer 395fea0f-4cbf-487d-90ef-d2241c5843c6" \
-i -H "Content-Type:application/json"
-X GET "https://test.usma.ibm.com:8443/restAPI/aliasListing/?groupTypeDescLike=IP \
&&aliasValueLike=%25%C%25"
```

This command provides the following JSON output:

```
HTTP/1.1 200 OK
X-FRAME-OPTIONS: SAMEORIGIN
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Date: Fri, 18 Jan 2019 20:02:59 GMT
Server: SQL Guard
[
  {
    "groupType": "Server IP", "DbValue": "5.6.7.8", "AliasValue": "C1" }
  ,
  {
    "groupType": "Server IP", "DbValue": "5.6.7.7", "AliasValue": "C2" }
  ,
  {
    "groupType": "Server IP", "DbValue": "5.6.7.6", "AliasValue": "C3" }
]
```

Related concepts

- [Aliases](#)

Related reference

- [create alias](#)
- [delete alias](#)
- [update alias](#)

list_all_reports

Run this command to output a list of all reports defined on the (specified) system.

This API is available in Guardium V10.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/list_all_reports
```

GuardAPI syntax

```
list_all_reports parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To output a list of all reports on the system on which you enter the command:

```
grdapi list_all_reports
```

Sample response:

```
##### Report Title #####
Command Details
Object Details
Field Details
Open Sessions
Open Sessions Monitor
DDL Commands
Sensitive Objects Usage
Sensitive Objects List
Administration Objects Usage
Administrative Commands Usage
One User One IP
Admin Users Login
Calls to procs with Buffer Overflow
DML Execution on Sensitive Objects
DML Execution on Administrative Objects
User Activity Summary
Client IP Activity Summary
Object Activity Summary
Open Sessions Graphical
Open Sessions By IP
Open Sessions Graphical Monitor
Admin Users Login Graphical
DDL Distribution
Sessions List
Commands List
Objects List
Fields List
Exceptions By Type
Exceptions Distribution
Exceptions Monitor
Exceptions Distribution List
Number of db per type
DB Server List
Logged Threshold Alerts
Logged R/T Alerts
Generated Alert Notifications
Exception Count
Policy Violation Count
Session Count
SQL Count
Number Of Active Processes
```

Outstanding Audit Process Reviews
Pre Defined Oracle Users access
Aggregation/Archive Log
User Activity Audit Trail
Guardium Logins
Detailed Guardium User Activity
Failed User Login Attempts
DB Predefined Users Login
Servers Accessed
New SQL Statements
SQL Errors
DML Executions Per Day
Sessions By Server Type
Activity By Client IP
MS-SQL Replication Procedures Call
MS-SQL Security Procedures Call
MS-SQL System Procedures Call
ALTER Commands Execution
CREATE Commands Execution
DROP Commands Execution
BACKUP Commands Execution
DBCC Commands Execution
GRANT Commands Execution
REVOKE Commands Execution
KILL Commands Execution
RESTORE Commands Execution
Sessions By Server IP
Sessions By Client IP
Sessions By User
Sessions By Source Program
Sessions Details By Server
Exceptions By Server
Exceptions By Client
Exceptions By User
Exceptions Details
Scheduled Jobs Exceptions
Users To-Do List
Long Running Queries
Throughput
Primary Guardium Host Change Log
Configuration Change History
Definitions Export/Import Log
Throughput-Chart
System/Security Activities
Dropped Requests
Rogue Connections
User Comments
Databases Discovered
Guardium Group Details
Values Changed
Values Changed Details
EBS Application Access
EBS Processes Database Access
Terminated Users Logins
Active Users Last Login
Terminated Users Failed Login Attempts
Archive Candidates
Active Users with no Activity
PSFT Application Access
PSFT Processes Database Access
User - Role
All Roles - User
All Roles - Application Access
All Guardium Applications - Role
Policy Violations
Open Incidents
Policy Violations List with Severity Details
Policy Violations / Incident Management
Open Incidents / Incident Management
Open Incidents / To do list
Windows File Share Activity
Hourly Access Details
SAP Application Access
SIEBEL Application Access
CAS Change Details
CAS Saved Data
CAS Templates
CAS Host History
CAS Instances
CAS Instance Config
TCP Exceptions
Catalog View
Location View
Used By View
S-TAP Status
Installed Policy Details
Inactive S-TAPs Since
Full SQL By Client IP
Full SQL By DB User
Guardium Job Queue
Executed DMLs On Sensitive Objects
Access to Sensitive Objects
Client IPs Activity
Policy Violations Details
Exceptions Type Distribution
Failed Login Attempts

Returned SQL Errors
Admin Users Sessions
DB Predefined Users Sessions
Use of Administrative Commands
Use Of Administrative Objects
Execution of DML Commands on Administrative Objects
Execution Of BACKUP Commands
Execution of RESTORE Commands
Execution of REVOKE Commands
Execution Of KILL Commands
Execution of DBCC Commands
Execution of GRANT Commands
Execution Of CREATE Commands
Execution Of DDL Commands
Distribution Of DDL Commands
Execution Of ALTER Commands
Execution Of DROP Commands
Activity Summary By Client IP
Detailed Sessions List
Commands Execution Summary
Objects Access Summary
Object Access By Client
Queries By Execution Time
DB Server Throughput
DB Server Throughput-Chart
EF - Logon
EF - Logoff
EF - Exception
EF - SQL Summary
EF - SQL Detail
DataSource Version History
Flat Log List
Buff Usage Monitor
No Traffic
Data-Sources
Request Rate
CPU Usage
Installed Patches
S-TAP Status Monitor
Guardium API Exceptions
Tap Event Exceptions
My Restore Log
Parser Exceptions
Scheduled Jobs
Group Members
ORA Accounts of ALTER SYSTEM
ORA Accounts with BECOME USER
ORA All Sys Priv and admin opt
ORA Obj And Columns Priv
ORA Object Access By PUBLIC
ORA Object privileges
ORA PUBLIC Exec Priv on SYS Proc
ORA Roles Granted
ORA Sys Priv Granted
ORA SYSDBA and SYSOPER Accounts
Classifier Results
Aggregation Errors
Logins to Guardium Appliance
Guardium Users - credentials
Policy Changes
Inspection Engine Changes
DataSource Changes
MYSQL DB Privils 40
MYSQL User Privils 40
MYSQL Host Privils 40
MYSQL Table Privils 40
MYSQL DB Privils 500
MYSQL User Privils 500
MYSQL Host Privils 500
MYSQL Table Privils 500
MYSQL DB Privils 502/up
MYSQL User Privils 502/up
MYSQL Host Privils 502/up
MYSQL Table Privils 502/up
DB2 Column Level Privils
DB2 DB Level Privils
DB2 Index Level Privils
DB2 Package Level Privils
DB2 Table Level Privils
DB2 Priv Summary
SYBASE Object Privils By DB Account
SYBASE Sys Priv And Role Granted To User
SYBASE Role Granted To User And Sys Privils Granted
SYBASE Object Access By Public
SYBASE Execute Priv On Proc Func To Public
SYBASE Accounts With Sys Or Sec Admin Roles
SYBASE Obj Col Privils Granted With Grant
SYBASE Role Granted To User
Informix Object Privils By DB Account
Informix Sys Priv And Role Granted To User
Informix Sys Priv And Role Granted To User Role
Informix Object Grant To Public
Informix Execute Priv On Proc Func To Public
Informix Account With Dba Privilege
Informix Obj Col Privils Granted With Grant
Informix Role Granted To User/Role

Microsoft SQL Server 2000 Obj Privs By Non-Default Sys User - Deprecated
Microsoft SQL Server 2000 Role/Sys Privs Granted To User - Deprecated
Microsoft SQL Server 2000 Role/Sys Privs Granted To User And Role - Deprecated
Microsoft SQL Server 2000 Object Access By PUBLIC - Deprecated
Microsoft SQL Server 2000 Exec Priv On Sys Proc Func To Public - Deprecated
Microsoft SQL Server 2000 account of db_owner db_securityadmin role - Deprecated
Microsoft SQL Server 2000 Srv Account of sys/server/security admin - Deprecated
Microsoft SQL Server 2000 Obj Col Privs Granted With Grant - Deprecated
Microsoft SQL Server 2000 Role Granted To User And Role - Deprecated
Microsoft SQL Server Obj Privs By Non-Default Sys User
Microsoft SQL Server Role/Sys Privs Granted To User
Microsoft SQL Server Role/Sys Privs Granted To User And Role
Microsoft SQL Server Object Access By PUBLIC
Microsoft SQL Server Exec Priv On Sys Proc Func To Public
Microsoft SQL Server Account Of db_owner db_securityadmin Role
Microsoft SQL Server Srv Account of sys/server/security admin
Microsoft SQL Server Obj Col Privs Granted With Grant
Microsoft SQL Server Role Granted To User And Role
Audit Process Log
Number of outstanding audit process reviews
Audit processes - Active/Inactive
Outstanding waiting reviews
Number of items in to-do lists
Number of open incidents
Critical failed tests
Number of failed critical tests
Access policy violations
Classifier policy violations
Number of access policy violations
Number of classifier policy violations
Backup number
Backups attempted
Number of installed policies
Purges attempted
Purge number
Archives attempted
Archive results attempted
Archive number
Archive results number
Groups Usage Report
Count Of Data-Sources with No VA Results
List Of Data-Sources with No VA Results
Count Of Host That Ceased To Be Monitored
Number Of Inactive S-TAPs
Security Assessment Export
Servers Associated
Datasources Associated
Application Objects Summary
CPU Tracker
Event Status Transition
Outstanding Events
Servers Not Associated
Datasources Not Associated
Discovered Instances
GIM Installed Modules
Teradata Obj Privs By Account
Teradata Sys Privs And Roles Granted To Users
Teradata Roles Granted To Users And Roles
Teradata Sys Privs And Role Granted
Teradata Obj and System Privs Granted to Public
Teradata Obj Privs Granted With Granted Option
Teradata Exec Privs On System DB Obs To Public
Teradata System and Security Admin Privs Granted
Logging collectors
Active S-TAPs Changed
Netezza Obj Privs by DB User name
Netezza Admin Privs by DB User name
Netezza Group/Role Granted To User
Netezza Obj Privs By Group
Netezza Admin Privs By Group
Netezza Admin Privs By DB User name Group
Netezza Obj Privs Granted
Netezza Admin Privs Granted
Netezza Global Admin Priv To Users and Groups
Netezza Global Obj Priv To Users and Groups
Query Entities & Attributes
Connections Quarantined
PostgreSQL Priv On Databases Granted To Public User Role With Or Without Granted Option
PostgreSQL Priv On Language Granted To Public User Role With Or Without Granted Option
PostgreSQL Priv On Schema Granted To Public User Role With Or Without Granted Option
PostgreSQL Priv On Tablespace Granted To Public User Role With Or Without Granted Option
PostgreSQL Role Granted To User Or Role
PostgreSQL Super User Granted To User Or Role
PostgreSQL Sys Privs Granted To User And Role
PostgreSQL Table View Sequence and Function privs Granted To Public
PostgreSQL Table View Sequence and Function Privs Granted With Grant Option
PostgreSQL Table View Sequence Function Privs Granted To Roles
PostgreSQL Table Views Sequence and Functions Privs Granted To Login
GIM Events List
Pending Audit Processes
Detailed Enterprise S-TAP View
Enterprise S-TAP View
DB Users Mapping List
Enterprise Buffer Usage Monitor
Restored Data
No Traffic By Server And Protocol

DW Dormant Objects
DW SELECT Object Access
DW EXECUTE Object Access
DW Dormant Objects-Fields
DW SELECT Object/Field Access
Available Patches
GIM Clients Status
CAS Deployment
S-TAP/Z Files
Default DB Users Enabled
Test Exceptions
Approved Tap Clients
IMS Data Access Details
IMS Access
IMS Event
IMS Object
Teradata Failed Logins
Export Sensitive Data To Discovery
Datamart Extraction Log
S-TAP Events
Managed Units
Classification Data Import
Enterprise aggregation/traffic information
Va Test Failing Since
Enterprise S-TAP association history
DB2 z/OS System Privileges Granted To GRANTEE With GRANT Option V10 And Higher
DB2 z/OS System Privileges Granted To GRANTEE With GRANT Option V9
DB2 z/OS System Privileges Granted To GRANTEE With GRANT Option V8
DB2 z/OS Object Privileges Granted To GRANTEE
DB2 z/OS Database Resource Granted To GRANTEE
DB2 z/OS Schema Privileges Granted To GRANTEE V8 Only
DB2 z/OS Schema Privileges Granted To GRANTEE V9 And Higher
DB2 z/OS Database Privileges Granted To GRANTEE
DB2 z/OS System Privileges Granted To GRANTEE V10 And Higher
DB2 z/OS System Privileges Granted To GRANTEE V9
DB2 z/OS System Privileges Granted To GRANTEE V8
DB2 z/OS Object Privileges Granted To PUBLIC
DB2 z/OS Executable Object Privileges Granted To PUBLIC
DB2 z/OS Database Resource Granted To PUBLIC
DB2 z/OS Schema Privileges Granted To PUBLIC
DB2 z/OS Database Privileges Granted To PUBLIC
DB2 z/OS System Privileges Granted To PUBLIC V10 And Higher
DB2 z/OS System Privileges Granted To PUBLIC V9
DB2 z/OS System Privileges Granted To PUBLIC V8
DB2 z/OS Object Privileges Granted To GRANTEE With GRANT Option
DB2 z/OS Database Resource Granted To GRANTEE With GRANT Option
DB2 z/OS Schema Privileges Granted To GRANTEE With GRANT Option V8 Only
DB2 z/OS Schema Privileges Granted To GRANTEE With GRANT Option V9 And Higher
DB2 z/OS Database Privileges Granted To GRANTEE With GRANT Option
ORA Roles Granted 8/9
ORA All Sys Priv and admin opt 8/9
ORA Sys Priv Granted 8
Unit Utilization
Unit Utilization Distribution
Unit Utilization details
Object Last Referenced
DB2 for i S-TAP Status
DB2 for i S-TAP configuration
Sybase IQ Object Privileges By DB User
Sybase IQ Object Privileges By Group
Sybase IQ System Authority And Group Granted To User
Sybase IQ System Authority And Group Granted To Users And Groups Grantee
Sybase IQ Object Access By Public
Sybase IQ Execute Privilege On Procedure and Function To PUBLIC
Sybase IQ User Group With DBA/Perms Admin/User Admin/Remote DBA database authority
Sybase IQ Table View Priv Granted With Grant
Sybase IQ Group Granted To User And Group
Sybase IQ Login Policy For User And Group With Login Option Setting
S-TAP Last Response
DATA SET Access
Utilization Thresholds
DATA SET Detailed Access
VSAM RLM
Custom Table Upload Log
Hadoop - Hue/Beeswax Report CDH3
Hadoop - MapReduce Report
Excessive Errors per Period
Privileged Account Utilization
Privileged User Access of Business Objects
Users Inactive Since
Hadoop - HBase Report
Hadoop - HDFS Report
Hadoop - Unauthorized MapReduce Jobs
Hadoop - BigInsights MapReduce Report
Hadoop - Exception Report
Hadoop - Full Message Details report
Optim - Failed Request Summary per Optim Server
Optim - Request Execution per User
Optim - Request Execution per Optim Server
Optim - Table Usage Details
Optim - Request Log
Optim - Table Usage Summary
Optim - Request Summary
Unit Utilization Daily Summary
Aggregation/Archive Detail Log
Aggregation/Archive Debug Log

Aggregation/Archive Fail Log
Connection Profiling List
Use of Privilege Accounts to Create a New Login
Accounts Created and Deleted within a Short Period
Access Direct from Extranet/DMZ
Slow queries
Excessive Failed Attempts to Grant
Use of Application Accounts by Other than Application
Top Massive Grants
CIS vulnerability
Compliant(Pass) Results
CVE compliance
DataSource Status
Failed Vulnerability Results
STIG compliance
DB2 z/OS zSecure Database Privileges Granted To GRANTEE
DB2 z/OS zSecure Database Privileges Granted To PUBLIC
DB2 z/OS zSecure Groups Granted To User
DB2 z/OS zSecure JAR File Resource Privileges Granted To Grantee
DB2 z/OS zSecure Package privileges granted to grantee
DB2 z/OS zSecure Package Privileges Granted To PUBLIC
DB2 z/OS zSecure Plan Privileges Granted To Grantee
DB2 z/OS zSecure Plan Privileges Granted To PUBLIC
DB2 z/OS zSecure Routine Privileges Granted To Grantee
DB2 z/OS zSecure Routine Privileges Granted To PUBLIC
DB2 z/OS zSecure Sequence Privileges Granted To Grantee
DB2 z/OS zSecure Storage Resource Privileges Granted To Grantee
DB2 z/OS zSecure System Privileges Granted To GRANTEE
DB2 z/OS zSecure System Privileges Granted To PUBLIC
DB2 z/OS zSecure Table And View Privileges Granted To Grantee
DB2 z/OS zSecure Table And View Privileges Granted To PUBLIC
DB2 z/OS zSecure Tablespace Resource Privileges Granted To Grantee
Blu Discovered Sensitive Objects
DB2 for i SQL activity
DB2 for i Exception
User Defined Extraction Log
Unauthenticated GIM Clients
ORA Object Dependencies
Microsoft SQL Server 2005 Object Dependencies
Sybase IQ Object Dependencies
Microsoft SQL Server Object Dependencies
SYBASE Object Dependencies
Informix Object Dependencies
DB2 Table View Dependencies
DB2 Trigger Dependencies
DB2 Routine Dependencies
DB2 for i 6.1 Object Privileges Granted To Grantee
DB2 for i 7.1 Object Privileges Granted To Grantee
DB2 for i 6.1 Object Privileges Granted To PUBLIC
DB2 for i 7.1 Object Privileges Granted To PUBLIC
DB2 for i Executable Object Privileges Granted To PUBLIC
DB2 for i 6.1 Object Privileges Granted To Grantee With GRANT
DB2 for i 7.1 Object Privileges Granted To Grantee With GRANT
DB2 for i Group Granted To User
DB2 for i Special Authorities Privileges Granted To GRANTEE
Hadoop - Yarn Job Report
Hadoop - Permissions Report
Hadoop - Sensitive Data activity report
Hadoop - Privilege users accessing sensitive objects
Hadoop - User Login
Hadoop - Unauthorized Yarn Job report
Hadoop - Privilege user Activity Report
Hadoop - User sessions
Guardium for Application Policy Violations
Guardium for Application Access
Analytic (Extraction)-Distributed
Available VA tests
Assessment summary
Inactive STAP
SAP HANA Analytical priv granted to grantee
SAP HANA App Privilege granted to grantee
SAP HANA Sys priv granted to grantee
SAP HANA DB Object priv granted to grantee
SAP HANA Exec Objects priv granted to PUBLIC
SAP HANA Object priv granted to grantee with GRANT OPTION
SAP HANA Object privileges granted to PUBLIC
SAP HANA Role granted to grantee
S-TAP Verification
Inactive Inspection Engines
Analytic Outliers Summary By Date
Analytic Outlier Details List
Analytic Outliers Summary By Date - enhanced
Analytic Outliers Details List - enhanced
Hadoop - Hue/Beeswax Exception Report
hadoop Hue/Beeswax Report
Job Dependencies
Job Dependencies Events
Locator
Failed User Login Attempts - Distributed
Aggregation/Archive Log - Distributed
SQL Errors - Distributed
Scheduled Jobs Exceptions - distributed
Scheduled Jobs - distributed
SOX - Financial Server IPs
SOX - Financial DBs
SOX - Financial Applications to DB Servers Map

SOX - Financial Applications Active Users
SOX - Financial DB Administrators
SOX - Source Programs Accessing financial Data
SOX - DB Protocol Version Used by source Programs
SOX - SQL Errors on Financial Data
SOX - Financial Data Access by Unauthorized Applications
SOX - Failed User Login Attempts
SOX - Exception Monitor
SOX - Logins to SQL-Guard Server
SOX - One User One IP
SOX - After Hours Access to Financial Data
SOX - Unauthorized User ID Usage
SOX - Login Failures by Server IP
SOX - DDL Activity on Financial DBs
SOX - DML Activity on Financial Data by Administrators
SOX - Select Activity on financial Data by Administrators
SOX - Unauthorized Client IP Activity on Financial Data
SOX - SQL Errors
SOX - Access Management: GRANT & REVOKE Commands
SOX - DDL Distribution
SOX - DML Distribution
SOX - Client IP Activity Summary on Financial Data
SOX - DB User Activity
SOX - Sessions by Financial Server IPs
SOX - Financial Object Access
SOX - User Activity Audit Trail
PCI - Cardholder Server IPs
PCI - Cardholder DBs
PCI - Database Clients to Servers Map
PCI - Cardholder Database Active Users
PCI - Cardholder DB Administrators
PCI - Authorized Source Programs
PCI - Shared Accounts
PCI - Shared Accounts Graphical
PCI - Activity by Root / Admin
PCI - Unauthorized Application Access
PCI - Cardholder Sensitive Objects
PCI Access to cardholder data
Basel II - Financial Server IPs
Basel II - Financial DBs
Basel II - Financial Applications to DB Servers Map
Basel II - Financial Applications Active Users
Basel II - Financial DB Administrators
Basel II - Source Programs Accessing financial Data
Basel II - DB Protocol Version Used by source Programs
Basel II - SQL Errors on Financial Data
Basel II - Financial Data Access by Unauthorized Applications
Basel II - Failed User Login Attempts
Basel II - Exception Monitor
Basel II - Logins to SQL-Guard Server
Basel II - One User One IP
Basel II - After Hours Access to Financial Data
Basel II - Unauthorized User ID Usage
Basel II - Login Failures by Server IP
Basel II - DDL Activity on Financial DBs
Basel II - DML Activity on Financial Data by Administrators
Basel II - Select Activity on Financial Data by Administrators
Basel II - Unauthorized Client IP Activity on Financial Data
Basel II - SQL Errors
Basel II - Access Management: GRANT & REVOKE Commands
Basel II - DDL Distribution
Basel II - DML Distribution
Basel II - Client IP Activity Summary on Financial Data
Basel II - DB User Activity
Basel II - Sessions by Financial Server IPs
Basel II - Financial Object Access
Basel II - User Activity Audit Trail
Data Privacy - Admin Access to Sensitive Data
Data Privacy - Servers Accessing Sensitive Objects
Data Privacy - Applications to DB Servers Access Map
Data Privacy - Non Privileged Active Users
Data Privacy - Access Trail To Sensitive Data
Data Privacy - Logging Attempts Failure
Data Privacy - Unauthorized Application Access
Analytic User Feedback
Enterprise Stap Verification
Files Privileges
Files Count Of Activity Per Server
Files Count Of Activity Per Client
Files Count Of Activity Per User
Files Crawler Configuration
Unique DB User and Server
Unique DB User and Server datamart
Per User Compliance
Per Server Compliance
Masking Engine Monitor
IMS Checkpoint Results
Enterprise Load Balancer Events
Classification Process Log
Export: Access Log
Export: Session Log
Export: Exception Log
Export: Full SQL
Export: Group Members
Export: Policy Violations
Load Balancer

File Activities
NAS File Activities
SharePoint File Activities
Queries Running Long Time
Suspected SQL Injection Cases
Suspected malicious STP Cases
Malicious STP Case Symptoms
SQL Injection Case Symptoms
File Entitlement
Admin Dashboard VA stats - Distributed
Admin Dashboard TODO list stats - Distributed
S-TAP and External S-TAP Statistics
Entitlement Recommendation
Entitlement User/Role
Quick Installation
Appliance Settings
GDPR - Higher Risk SQL Errors
GDPR - Policy Violations
GDPR - Data Subject Delete Audit Trail
GDPR - Data Subject Rectification Audit Trail
GDPR - Data Subject Access Audit Trail
GDPR and GDPR z/OS - Discovered Personal Data Objects
GDPR - Personal Data Objects Audit Trail
GDPR - Personal Data Servers Audit Trail
GDPR - Access Management GRANT and REVOKE Commands
GDPR - Login Failure to Personal Data DBs
GDPR - After Hours Access to Personal Data
GDPR - Unauthorized Application Access
GDPR - Unauthorized Users Access
GDPR - Personal Data Definitions
GDPR - Administrative Activity on Personal DBs
GDPR - DDL Activity of Personal DBs
GDPR z/OS - DDL Activity of Personal DBs
GDPR z/OS - Unauthorized User Access
GDPR z/OS - Unauthorized Application Access
GDPR z/OS - Login Failures to Personal Data DB
GDPR z/OS - Data Subject Access Audit Trail
GDPR z/OS - Data Subject Rectification Audit Trail
GDPR z/OS - Data Subject Delete Audit Trail
GDPR z/OS - Access Management GRANT and REVOKE Commands
GDPR z/OS - Administrative Acitivity on Personal DBs
GDPR z/OS - After Hours Access to Personal Data
GDPR z/OS - Personal Data Servers Audit Trail
GDPR z/OS - Personal Data Objects Audit Trail
GDPR z/OS - Policy Violations
GDPR z/OS - Higher Risk SQL Errors
BigData Intelligence - Discovered Personal Data Objects
BigData Intelligence - Unauthorized Application Access
BigData Intelligence - Unauthorized Users Access
BigData Intelligence - High Risk SQL Errors
BigData Intelligence - Personal Data Servers Audit Trail
BigData Intelligence - Personal Data Objects Audit Trail
BigData Intelligence - Policy Violations
BigData Intelligence - Administrative Activity of Personal DBs
BigData Intelligence - Login Failure to Personal Data DB
BigData Intelligence - Data Subject Rectification Audit Trail
BigData Intelligence - Data Subject Delete Audit Trail
BigData Intelligence - Data Subject Access Audit Trail
BigData Intelligence - Access Management GRANT & REVOKE
BigData Intelligence - DDL Activity of Personal DBs
BigData Intelligence - DML Execution on Sensitive Objects
BigData Intelligence - Massive Operation on Sensitive Data
BigData Intelligence - Exceptions by Server
BigData Intelligence - Exceptions: Top Servers
BigData Intelligence - Failed User Login Attempts
BigData Intelligence - Grants by DB user name for a given server and database
BigData Intelligence - Top massive grants
BigData Intelligence - After Hours Access to Personal Data
Directory Entitlement
Analytic Status
Guardium entitlement consolidation report (using ILMT)
GDPR FAM - After Hours Access to Personal Data
GDPR FAM - Sensitive Files Audit Trail
GDPR FAM - Sensitive Files Audit Trail (Count of requests)
GDPR FAM - Data Subject Access Audit Trail
GDPR FAM - Data Subject Delete Audit Trail
GDPR FAM - Data Subject Rectification Audit Trail
GDPR FAM - File Operation Activity
GDPR FAM - Unauthorized Application Access
GDPR FAM - Unauthorized Users Access
GDPR FAM - Policy Violations
GDPR FAM - Sensitive Files
GDPR FAM - File Entitlement
Disabled users
Health Check Log
Health Check Log - Details
Enterprise No Traffic Alert
Policy Violations List
Enterprise S-TAPs Changed
SQL per server
Count of DB Type
Guardium - add/remove users
Managed Units Alert
Count of failed VA tests per server
Guardium - Credential Related Activity
Count of client IP per server

Count of DB traffic type per server
Count of SQL errors per server
PCI Cardholder Object Access
Calls to xp% procedures
Count of failed login per server
Count of Sessions per server
Count of Users per server
CAS Template Configuration
Administrative Commands By User Dashboard-Distributed
Error Code Analysis for Dashboard-Distributed
Most Active Client Dashboard-Distributed
Unique DB User and Server-Distributed
Active Risk Spotter - Risky Users Scores
Risky Users - Connection Profiling List
Risky Users - SQL Errors
Risky Users - Policy Violation
Active Risk Spotter - Risky User
Active Risk Spotter - Watchlist Snapshot
Import Definitions Log
Import Definitions Detail Log
GIM Certificate Deployment Status
System Parameters Change Log
Failed logins by database user - Distributed
Failed high-risk commands by server IP - Distributed
Privileged users issuing administrative commands - Distributed
Most active clients by IP - Distributed
Threat Analytics Case for Analysis
Threat Analytics Closed Cases
Threat Analytics Open Cases
Threat Analytics Case Observations
Exception Types Missing DB User
Local Sessions Missing DB User
Remote Sessions Missing DB User
Latest Exceptions Missing DB User
KTAP Dropped Packets
Latest Sessions Missing DB User
Flat Log Requests
Sessions per Day
Sniffer Restarts
Session Types Missing DB User
Sessions Missing DB User Per Day
Test Detail Exceptions
Failed logins by database user
Failed high-risk commands by server IP
Most active clients by IP
Privileged users issuing administrative commands
Flat Log Process Status
Outlier Mining Enable/Disable History
Host References
Assessment Tests
Assessment Datasources
Assessment Roles Allowed
CCPA - Higher Risk SQL Errors
CCPA - Policy Violations
CCPA - Data Subject Delete Audit Trail
CCPA - Data Subject Rectification Audit Trail
CCPA - Data Subject Access Audit Trail
CCPA and CCPA z/OS - Discovered Personal Data Objects
CCPA - Personal Data Objects Audit Trail
CCPA - Personal Data Servers Audit Trail
CCPA - Access Management GRANT and REVOKE Commands
CCPA - Login Failure to Personal Data DBs
CCPA - After Hours Access to Personal Data
CCPA - Unauthorized Application Access
CCPA - Unauthorized Users Access
CCPA - Personal Data Definitions
CCPA - Administrative Activity on Personal DBs
CCPA - DDL Activity of Personal DBs
CCPA z/OS - DDL Activity of Personal DBs
CCPA z/OS - Unauthorized User Access
CCPA z/OS - Unauthorized Application Access
CCPA z/OS - Login Failures to Personal Data DB
CCPA z/OS - Data Subject Access Audit Trail
CCPA z/OS - Data Subject Rectification Audit Trail
CCPA z/OS - Data Subject Delete Audit Trail
CCPA z/OS - Access Management GRANT and REVOKE Commands
CCPA z/OS - Administrative Acitivity on Personal DBs
CCPA z/OS - After Hours Access to Personal Data
CCPA z/OS - Personal Data Servers Audit Trail
CCPA z/OS - Personal Data Objects Audit Trail
CCPA z/OS - Policy Violations
CCPA z/OS - Higher Risk SQL Errors
Failed logins by database user for application - Distributed
Failed high-risk commands by server IP for application - Distributed
Privileged users issuing administrative commands for application - Distributed
Most active clients by IP for application - Distributed
Failed logins by database user for application
Failed high-risk commands by server IP for application
Most active clients by IP for application
Privileged users issuing administrative commands
Analytic Outlier Details
Analytic Outliers Summary
External Tickets
Query Execution Log
Threat Finder Run Log
Analytic Threat Case Details

```

Assessment Test Results by Datasource Severity
CCPA - Personal Data Objects Audit Trail-Distributed
CCPA z/OS - Personal Data Objects Audit Trail-Distributed
Data Set z/OS - Sensitive Object Activity
Data Set z/OS - Privileged User Activity
DB2 z/OS - Sensitive Object Activity
DB2 z/OS - Privileged User Activity
IMS z/OS - Sensitive Object Activity
IMS z/OS - Privileged User Activity
ok

```

Related concepts

- [Reports](#)

Related reference

- [Reporting and report generation APIs](#)

list_allowed_db_by_user

This command returns the available User-DB associations by the user's name.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/allowed_db
```

GuardAPI syntax

```
list_allowed_db_by_user parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| userName | String | Required. The name of the user. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapi list_allowed_db_by_user userName=Fred
```

Sample output

```
ID=0
Record Id = 1, Id = 20000, Type: USER, Instance: TEST
Servers associated with: Fred
Server Instance Access
-----
```

Related concepts

- [Data Security - User Hierarchy and Database Associations](#)

Related reference

- [create_allowed_db](#)

list_api_key

12.1 and later This command lists the API keys. If the logged-in user has an accessmgr role, all the API keys that are associated with the Guardium system are displayed. If the logged-in user does not have an accessmgr role, only the API keys that are associated with the user are displayed.

GuardAPI syntax

`list_api_key`

This API takes no parameters.

list_approved_stap_client

This command returns details on the approved S-TAP clients databases; database(s) whose S-TAPs are allowed (certified) to access and communicate with the specified Guardium® system.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/approved_stap_client
```

GuardAPI syntax

`list_approved_stap_client parameter=value`

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To view the databases certified to communicate with the Guardium system on which you enter the command:

```
grdapic list_approved_stap_client
```

Related tasks

- [Allow \(approve\) S-TAP connection to Guardium \(S-TAP Certification\)](#)

Related reference

- [S-TAP and inspection engine APIs](#)

list_assessment_tests

This command displays the list of tests for the security assessment.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/assessment_test
```

GuardAPI syntax

```
list_assessment_tests parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|-------------|
| assessmentDescription | String | |

Example

```
grdapi list_assessment_tests
```

list_assessments

This command lists security assessments.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/assessment
```

GuardAPI syntax

```
list_assessments parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|-------------|
| assessmentDescription | String | |

Example

```
grdapi list_assessments
```

list_associated_stap_mu_groups

This API returns a list of the managed unit groups of group type STAP that are associated with the specified Guardium system.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/list_associated_stap_mu_groups
```

GuardAPI syntax

```
list_associated_stap_mu_groups parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------------|------------|---|
| printFailoverGroupInfo | Boolean | If set to 1, includes failover group information. For more information, see assign_load_balancer_groups .
Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To view the list of the managed unit groups of type S-TAP that are associated with the Guardium system on which you enter the command:

```
grdapi list_associated_stap_mu_groups
grdapi list_associated_stap_mu_groups printFailoverGroupInfo=1
```

Related reference

- [S-TAP and inspection engine APIs](#)

list_audit_processes

This command displays a list of available audit processes.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/audit_process
```

GuardAPI syntax

```
list_audit_processes parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Guard API example

```
grdapi list_audit_processes
ID=0
Active Risk Spotter
Appliance Monitoring
Open Threat Analytics Cases
Suspected malicious STP Cases
Suspected SQL Injection Cases
Table Last Referenced
```

Related reference

- [execute_auditProcess](#)

list_autodetect_processes

Use this command to output the names of all the auto-discovery processes.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/autodetect_processes
```

GuardAPI syntax

```
list_autodetect_processes parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To list the auto-discovery processes:

```
grdapic list_autodetect_processes
```

Related concepts

- [Database auto-discovery](#)

Related reference

- [Auto-discovery APIs](#)

list_autodetect_tasks_for_process

Use this command to output a list of all tasks associated with a specified auto-discovery process.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/autodetect_tasks_for_process
```

GuardAPI syntax

```
list_autodetect_tasks_for_process parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------|------------|--|
| process_name | String | Required. Name of the auto-discovery process |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To list all tasks associated with the process myProcess:

```
grdapic list_autodetect_tasks_for_process process_name=myProcess
```

Related concepts

- [Database auto-discovery](#)

Related reference

- [Auto-discovery APIs](#)

list_available_test_notes

This API is available in Guardium v11.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/available_test_notes
```

GuardAPI syntax

```
list_available_test_notes parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| datasourceType | String | Required. For valid values, call <code>list_available_test_notes</code> from the command line with <code>--help=true</code> . |
| testDescription | String | Required. |

list_available_tests

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/available_test
```

GuardAPI syntax

```
list_available_tests parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|--|
| datasourceType | String | Required. For valid values, call <code>list_available_tests</code> from the command line with <code>--help=true</code> . |

| Parameter | Value type | Description |
|-----------------|------------|-------------|
| testDescription | String | |

list_aws_secrets_manager_config

Use this command to list one or more AWS Secrets Manager configurations.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/aws_secrets_manager
```

GuardAPI syntax

```
list_aws_secrets_manager_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| name | String | |

Examples

```
grdapli list_aws_secrets_manager_config name="GRDAPI IAM-Instance-Profile"
grdapli list_aws_secrets_manager_config name="GRDAPI IAM-Role"
grdapli list_aws_secrets_manager_config name="GRDAPI Security-Credentials"
```

The following example lists all AWS Secrets Manager configurations:

```
grdapli list_aws_secrets_manager_config
```

list_cas_host_instances

This command returns a list of the Configuration Auditing System (CAS) host instances. You must specify either the `hostName` or the `datasourceName`.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/cas_host_instance
```

GuardAPI syntax

```
list_cas_host_instances parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| datasourceName | String | The name of a data source with host instances. |
| hostName | String | The host name or IP address. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • <code>all_managed</code>: execute on all managed units but not the central manager • <code>all</code>: execute on all managed units and the central manager • <code>group:<group name></code>: execute on all managed units identified by <code><group name></code> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

The following example lists the host instance that is associated with an IP address:

```
grdapic list_cas_host_instances hostName=9.70.150.111
```

Which returns the following information:

```
Id, dataSourceName(#), dataSourceName, templateSetLabel(#), templateSetLabel, hostName, osType, dbType  
c0d2327c8dd550549f2579ab44819a54c3db5e6a, 20002, System (9.70.150.111), 16, Default Unix Template Set, 9.70.150.129, UNX, N_A  
ok
```

list_cas_hosts

This command returns a list of the Configuration Auditing System (CAS) hosts. You can filter the returned list by operating system.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/cas_host
```

GuardAPI syntax

```
list_cas_hosts parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| osType | String | The operating system type can be either: <ul style="list-style-type: none">• UNIX: UNIX• WIN: Windows |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GuardAPI example

To return a list of all UNIX-based CAS hosts.

```
grdapic list_cas_hosts osType=UNIX
```

Example output:

```
hostName, osType  
9.70.150.159, UNIX  
9.70.150.160, UNIX  
9.70.150.129, UNIX  
9.98.171.216, UNIX  
ok
```

REST API example

To return a list of all UNIX-based CAS hosts.

```
curl -k -i --header "Authorization: Bearer 8ad14246-8815-4043-ab19-074d6bfcaad3"  
https://localhost:8443/restAPI/cas_host?osType=UNIX
```

Related reference

- [Configuration Auditing System \(CAS\) APIs](#)

list_cas_template_sets

This command returns a list of the Configuration Auditing System (CAS) template sets. You can filter the returned list by database, operating system, or both.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/cas_template_set
```

GuardAPI syntax

```
list_cas_template_sets parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| dbType | String | The database type.
If you enter a database type that is not supported (or you misspell it), Guardium displays a list of supported DBs.

To list templates that do not require a specific DB type, specify N_A. |
| osType | String | The operating system type can be either: <ul style="list-style-type: none">• UNIX: UNIX• WIN: Windows |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123.
IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GuardAPI example

To request a list of template sets on Windows for Oracle:

```
grdapic list_cas_template_sets osType=WIN dbType=Oracle
```

Example output:

```
Id, templateSetLabel, osType, dbType, Default, editable
17, Default Windows/Oracle Template Set, WIN, ORACLE, true, false
55, Default Windows/Oracle Template Set v8.0, WIN, ORACLE, true, false
34, Windows/Oracle Assessment, WIN, ORACLE, false, false
```

REST API example:

To list CAS template sets for Db2:

```
curl -k -i --header "Authorization: Bearer 8ad14246-8815-4043-ab19-074d6bfcaad3"
https://localhost:8443/restAPI/cas_template_set?dbType=DB2
```

Example output

```
[{"audit_config_template_set_id": 20001, "label": "cas_temp_set_001", "os_type": "UNIX", "db_type": "DB2", "default": "true", "editable": "true"}, {"audit_config_template_set_id": 20000, "label": "ddi", "os_type": "UNIX", "db_type": "DB2", "default": "true", "editable": "true"}]
```

```
}
```

Related concepts

- [Configuration Auditing System \(CAS\)](#)

Related reference

- [Configuration Auditing System \(CAS\) APIs](#)

list_cas_templates

This command returns a list of the templates within a specified Configuration Auditing System (CAS) template set.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/cas_template
```

GuardAPI syntax

```
list_cas_templates parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|---|
| templateSetLabel | String | Required. The name of the template set. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

To request a list of all templates in the template set named *tempSet*:

```
grdapi list_cas_templates templateSetLabel=tempSet
```

Example output:

```
ID=20001
Id, auditType, template, enabled, period, useMD5, saveData, isEditable
20000, FILE, templateTest, true, 3600, false, false, true
ok
```

REST API example

To list CAS templates by template set name:

```
curl -k -i --header "Authorization: Bearer 8ad14246-8815-4043-ab19-074d6bfcaad3"
https://localhost:8443/restAPI/cas_template?templateSetLabel=cas_temp_set_001
```

Example output:

```
[
  {
    "audit_config_template_id": 20002,
    "audit_type": "FILE",
    "template": "$DB2_HOME/sqllib/db2nodes.cfg",
    "enabled": "true",
    "period": 3600,
    "use_md5": "false",
    "save_data": "true",
```

```

        "is_editable": "true"
    },
    {
        "audit_config_template_id": 20001,
        "audit_type": "FILE",
        "template": "test.txt",
        "enabled": "true",
        "period": 3600,
        "use_md5": "false",
        "save_data": "true",
        "is_editable": "true"
    }
]

```

Related concepts

- [Configuration Auditing System \(CAS\)](#)

Related reference

- [Configuration Auditing System \(CAS\) APIs](#)

list_classifier_policy

This command lists information about classification policies, rules, and actions.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/classifier_policy
```

GuardAPI syntax

```
list_classifier_policy parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|--|
| actionName | String | |
| policyName | String | |
| recursive | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| ruleName | String | |

Examples

List information about a specific action:

```
grdapiclient list_classifier_policy policyName=access_policy ruleName=access_rule actionName=log_access
```

Recursively list information about all actions for a specific rule:

```
grdapiclient list_classifier_policy policyName=access_policy ruleName=access_rule recursive=1
```

Recursively list information about all actions for all rules in all policies:

```
grdapiclient list_classifier_policy recursive=1
```

list_classifier_process

This command list information about classification processes.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/classifier_process
```

GuardAPI syntax

```
list_classifier_process parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|--|
| datasourceType | String | Valid values: <ul style="list-style-type: none">• DOCUMENT• RELATIONAL Default = RELATIONAL |
| processName | String | |

Examples

List information about all processes:

```
grdapi list_classifier_process
```

List information about a specific process:

```
grdapi list_classifier_process processName=APITEST_Clps_10001_1
```

list_cloud_datasource_by_name

This command outputs the configured details on the specified datasource.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/cloud_datasource
```

GuardAPI syntax

```
list_cloud_datasource_by_name parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| name | String | Required. Cloud datasource defined in Guardium. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

Use this command to view details on the datasource named cloud9.

```
grdapi list_cloud_datasource_by_name name=cloud9
```

list_compatibility_modes

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/compatibility
```

GuardAPI syntax

```
list_compatibility_modes parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

list_computed_attribute

This API lists the computed attributes available for a specified entity.

Use this API to find information about an existing computed attribute that was created with the [create_computed_attribute](#) API.

This API is available in Guardium V11.4 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/list_computed_attribute
```

GuardAPI syntax

```
list_computed_attribute parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------------|------------|---|
| attributeLabelLike | String | All or part of the computed attribute name that appears in reports. |
| entityLabel | String | Required. The name of the main entity with which the attribute is associated, for example Session, Object, or FULL_SQL. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapi list_computed_attribute entityLabel="Object" attributeLabelLike="test"
```

Related reference

- [create_computed_attribute](#)

list_custom_table_ldap_imports

This command lists custom tables that were created to import data from LDAP.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/custom_data_ldap
```

GuardAPI syntax

```
list_custom_table_ldap_imports parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| tableName | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

list_cyberark_config

This command lists CyberArk configurations on your Guardium system.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/cyberark
```

GuardAPI syntax

```
list_cyberark_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| name | String | The name of an existing CyberArk configuration. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

list_datasourceRef_by_id

This command lists all datasource references for a specific object of a specific application type. The object and application type are referenced by identification keys.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/datasource_ref
```

GuardAPI syntax

```
list_datasourceRef_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| appId | Integer | Required. Identifies the application type.
Valid values: <ul style="list-style-type: none">• 8 (security assessment)• 47 (custom tables)• 51 (classifier) |
| objId | Integer | Required. Identifies an instance of the specified appId type. For example, if <code>appId=51</code> , objId is the identification key of a classification process. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

```
grdapi list_datasourceRef_by_id appId=13 objId=1
```

list_datasourceRef_by_name

This command lists all datasource references for a specific object of a specific application type. The object and application type are referenced by name.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/datasource_ref
```

GuardAPI syntax

```
list_datasourceRef_by_name parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|---|
| application | String | Required. Identifies the application type. For valid values, call <code>list_datasourceRef_by_name</code> from the command line with <code>--help=true</code> . |
| objName | String | Required. For valid values, call <code>list_datasourceRef_by_name</code> from the command line with <code>--help=true</code> . |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

list_datasource_by_id

This command displays a datasource definition identified by an identification key.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/datasource
```

GuardAPI syntax

```
list_datasource_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| id | Integer | Required. The identification key of the datasource to be listed. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Use this command to view details about a datasource with identification key 2:

```
grdapic list_datasource_by_id id=2
```

list_datasource_by_name

This command displays a datasource definition identified by name.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/datasource
```

GuardAPI syntax

```
list_datasource_by_name parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| name | String | Required. The datasource name. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Use this command to view details about a datasource with the name `chickenDB2`:

```
grdapi list_datasource_by_name name=chickenDB2
```

list_datasource_groupRef_by_id

List the datasource groups that are in security assessments, discovery scenarios, or custom tables.

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/datasource_group_ref
```

GuardAPI syntax

```
list_datasource_groupRef_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| appId | Integer | Required. For valid values, call <code>list_datasource_groupRef_by_id</code> from the command line with <code>--help=true</code> . |
| objId | Integer | Required. The object ID of the security assessment, discovery scenario, or custom table. |

list_datasource_groupRef_by_name

List the datasource groups that are in security assessments, discovery scenarios, or custom tables.

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/datasource_group_ref
```

GuardAPI syntax

```
list_datasource_groupRef_by_name parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|--|
| application | String | Required. For valid values, call <code>list_datasource_groupRef_by_name</code> from the command line with <code>--help=true</code> . |
| objName | String | Required. The name of the security assessment, discovery scenario, or custom table. |

list_datasource_group_hierarchy

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/datasource_group_listing
```

GuardAPI syntax

```
list_datasource_group_hierarchy parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| datasourceName | String | |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

list_datasource_group_members

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/datasource_group
```

GuardAPI syntax

```
list_datasource_group_members parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| groupName | String | Required. |

list_datasource_groups

This API is available in Guardium v11.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/datasource_group
```

GuardAPI syntax

```
list_datasource_groups parameter=value
```

list_db_drivers

This command lists the available database drivers.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/db_drivers
```

GuardAPI syntax

```
list_db_drivers parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapic list_db_drivers
```

list_db_drivers_by_details

This command details about the available database drivers.

The listed details include name, datasource class, driver class, URL, and datasource type ID.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/list_db_drivers_by_details
```

GuardAPI syntax

```
list_db_drivers_by_details parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapi list_db_drivers_by_details
```

list_db_user_mapping

This command returns the mappings between DB user and email address for real-time alerts.

You can use a percent (%) wildcard for all parameters.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/db_user_mapping
```

GuardAPI syntax

```
list_db_user_mapping parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| dbUserName | String | Required. The DB username. |
| emailAddress | String | Required. For real-time alerts, the email address that maps to the DB user. The at symbol (@) is required. |
| serverIp | String | Required. The server IP address. You can use % wildcards for any element in the IP address. For example: <ul style="list-style-type: none">• 192.168.2.%• 2620:1f7:807:%:920:% |
| serviceName | String | Required. The server name. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GuardAPI example

```
grdapi list_db_user_mapping serverIp=192.168.1.% serviceName=ora% dbUserName=hadrian emailAddress=hadrian.swall@company.com
```

Related concepts

- [Alerting rule actions](#)

Related reference

- [create_db_user_mapping](#)

list_ef_mapping

This command lists all external feed mappings or details about a specified mapping.

If run without any parameters, this function returns a list of all user-created mappings. If run with the reportName parameter, this function returns details of the specified mapping (such as the table and column names used by the external feed).

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/list_ef_mapping
```

GuardAPI syntax

```
list_ef_mapping parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| reportName | String | View details for the report mapping identified by reportName. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Use this command to view all user-created external feed mappings:

```
grdapi list_ef_mapping
```

Use this command to view details for the *Sessions per Day* mapping:

```
grdapi list_ef_mapping reportName="Sessions per Day"
```

list_ef_report

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/list_ef_report
```

GuardAPI syntax

```
list_ef_report parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

list_engine_config

Run this command to view the general inspection engine configuration. This configuration applies to all inspection engines that report to the specified Guardium system, and can be seen in the GUI Inspection Engine Configuration page.

You can change these settings either from the GUI Inspection Engine Configuration page or with the API update_engine_config.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/engine_config
```

GuardAPI syntax

```
list_engine_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To view the inspection engine configuration for the Guardium system on which you enter the command:

```
grdapi list_engine_config
```

Sample output:

```
ID=0
Inspection Engine Configuration
Default Capture Value OFF
Default Mark Auto Commit ON
Log Sequencing OFF
Log Exception Sql String ON
Log Records Affected OFF
Compute Avg. Response Time OFF
Inspect Returned Data OFF
Record Empty Sessions OFF
Parse XML OFF
Logging Granularity 60
Max. Hits per Returned Data 64
Ignored Ports List
Buffer Free 100%
ok
```

Related concepts

- [Inspection Engine Configuration](#)

Related reference

- [update_engine_config](#)
- [S-TAP and inspection engine APIs](#)

list_entry_location

This command returns a specific catalog entry if you include a file name. If you do not specify the file name, it returns details of all the catalog entries for this host and path.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/entry_location
```

GuardAPI syntax

```
list_entry_location parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| fileName | String | Specifies the file location for this archive location. If omitted, the command returns details of all the catalog entries on the specified hostname and path. |
| hostName | String | Required. The hostname or IP address. |
| path | String | Required. The path to the archive directory. <ul style="list-style-type: none">• Amazon S3: bucket name• IBM COS: bucket name• EMC Centera: Centera clipID• FTP: Specify the directory relative to the FTP account home directory.• SCP: Specify the directory as an absolute path.• IBM Cloud: Container• TSM: path |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GuardAPI example

```
grdapi list_entry_location path=/mnt/nfs/archive_results/ hostName=192.168.1.33
```

Related tasks

- [Data and Result catalogs](#)

Related reference

- [Archive, export, import, purge, and restore APIs](#)
- [Catalog entry APIs](#)

list_existing_job_dependencies

Run this command to output the jobs on which the specified job has dependencies.

This API is available in Guardium V10.1.4 and later.

GuardAPI syntax

```
list_existing_job_dependencies parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|-------------|
| jobTrigger | String | Required. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To output the jobs on which `DataMartExtractionJobTrigger_5` has dependencies:

```
grdapi list_existing_job_dependencies jobTrigger=DataMartExtractionJobTrigger_5
ID=0
##### RUNNABLE AUTO-EXEC DEPENDENCY #0 #####
JOB_CATEGORY=distributedReportExtraction
JOB_OBJECT=distributedReportExtraction
ok
```

Related concepts

- [Scheduling](#)
- [Job dependencies](#)

Related reference

- [Schedule and job dependencies APIs](#)

list_expiration_dates_for_restored_days

This command returns the expiration dates for all restored data.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/expiration_dates_for_restored_days
```

GuardAPI syntax

```
list_expiration_dates_for_restored_days parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
list_expiration_dates_for_restored_days
```

Related tasks

- [Managing stored data](#)

Related reference

- [Archive, export, import, purge, and restore APIs](#)

list_group_by_desc

This command displays the properties of a group identified by its description.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/group
```

GuardAPI syntax

```
list_group_by_desc parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| desc | String | Required. Identifies the group by its description. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

Use this command to list details about the group `A group`:

```
grdapic list_group_by_desc desc="A group"
```

list_group_by_id

This command displays the properties of a group identified by its identification key.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/group
```

GuardAPI syntax

```
list_group_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| id | Integer | Required. Identifies the group by its identification key. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Use this command to view details about the group with identification key `100003`:

```
grdapi list_group_by_id id=100003
```

list_group_members_by_desc

This command displays the members of a group identified by its description.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/group_members_by_group_desc
```

GuardAPI syntax

```
list_group_members_by_desc parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| desc | String | Required. Identifies the group by its description. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Use this command to list the members of the group `A group`:

```
grdapi list_group_members_by_desc desc="A group"
```

list_group_members_by_id

This command displays the members of a group identified by its identification key.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/group_members_by_group_id
```

GuardAPI syntax

```
list_group_members_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| id | Integer | Required. Identifies the group by its identification key. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Use this command to list the members of the group with identification key 100005:

```
grdapi list_group_members_by_id id=100005
```

list_groups

This API returns details about the groups defined in the local, or specified, Guardium system. The description does not include group members.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/group
```

GuardAPI syntax

```
list_groups parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| skipEmpty | Boolean | <p>Whether or not empty groups are returned. Valid values:</p> <ul style="list-style-type: none">• 0 (false)• 1 (true) <p>Default = 0 (false)</p> |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Typical output:

```

grdapi list_groups
ID=0
Group Id: 80, Description: "Administrative Programs", Application: "Public", Type: "SOURCE PROGRAM", Hierarchical: false,
Member Count: 0, Tuple Count: 1
Group Id: 254, Description: "All Failed Authorization", Application: "Public", Type: "DB Error Codes", Hierarchical: false,
Member Count: 7, Tuple Count: 1
Group Id: 17, Description: "ALTER Commands", Application: "Public", Type: "COMMANDS", Hierarchical: false, Member Count: 35,
Tuple Count: 1
Group Id: 192, Description: "Analytic Exclude DB User", Application: "Public", Type: "USERS", Hierarchical: false, Member
Count: 0, Tuple Count: 1
Group Id: 193, Description: "Analytic Exclude OS User", Application: "Public", Type: "USERS", Hierarchical: false, Member
Count: 0, Tuple Count: 1
Group Id: 194, Description: "Analytic Exclude Server IP", Application: "Public", Type: "Server IP", Hierarchical: false, Member
Count: 0, Tuple Count: 1

```

Related reference

- [Group APIs](#)

list_hashicorp_config

Use this command to view the list of HashiCorp configurations on your Guardium® system.

This API is available in Guardium V11.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/hashicorp
```

GuardAPI syntax

```
list_hashicorp_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| name | String | The name of the HashiCorp configuration. |

Examples

The following example lists the details of all available HashiCorp configurations:

```

grdapi list_hashicorp_config
ID=0
hashicorp_config_id: 1, name: "No SSL User and password API", auth_type: "Username & Password", vault_host_name: "hostname",
vault_port: 8300, user_name: "apps", password: "*****", use_ssl: "false"
hashicorp_config_id: 2, name: "SSL User and password API", auth_type: "Username & Password", vault_host_name: "hostname",
vault_port: 8500, user_name: "apps", password: "*****", use_ssl: "true"
ok

```

The following example lists the details of a specific HashiCorp configuration:

```

grdapi list_hashicorp_config name="SSL User and password API"
ID=0
hashicorp_config_id: 2, name: "SSL User and password API", auth_type: "Username & Password", vault_host_name: "hostname",
vault_port: 8500, user_name: "apps", password: "*****", use_ssl: "true"
ok

```

Related concepts

- [Datasource credential management APIs](#)

list_health_node

This command provides health and other information about the current machine. For a central manager, information also displays for all managed units.

For deployment health, the numbers are mapped as follows:

- -1 - Unavailable
- 0 - Healthy
- 1 - Unknown/Stale
- 2 - Medium severity
- 3 - High severity

This API is available in Guardium V10.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/list_health_node
```

GuardAPI syntax

```
list_health_node parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">all_managed: execute on all managed units but not the central managerall: execute on all managed units and the central managergroup:<group name>: execute on all managed units identified by <group name>host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Example

```
grdapi list_health_node
```

Sample output:

```
[{"id":0,"name":"my.system.com","unitHostIp":null,"type":"ag","patch":null,"status":0,"parent":"none","connectivity":0,"version":1}
```

list_imscheckpoint_records

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/ims_checkpoint
```

GuardAPI syntax

```
list_imscheckpoint_records
```

This API takes no parameters.

list_inspection_engines

This command lists all the defined inspection engines, and their configurations, on the specified S-TAP® host.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/inspection_engine
```

GuardAPI syntax

```
list_inspection_engines parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| stapHost | String | Required. IP or hostname of the S-TAP host. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| type | String | The type of inspection engine. One of: Windows: CouchDB, Db2®, Db2 Exit, Informix®, MongoDB, MS SQL, MySql, Oracle, PostgreSQL, Sybase; UNIX: Aster, Cassandra, CouchDB, Db2, Db2 Exit, exclude IE, FTP, GreenPlumDB, Hadoop, Hive, HTTP, Hue, IBM® iSeries, Impala, Informix, Informix Exit, Kerberos, MariaDB, MongoDB, MySql, Netezza®, Oracle, PostgreSQL, SAP HANA, Vertica, Sybase, Teradata, Vertica, or WebHDFS |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To view the inspection engines on the DB server with the IP 9.42.29.158:

```
grdapic list_inspection_engines stapHost=9.42.29.158
ID=7
S-TAP Host: 9.42.29.158 - Not Active
Inspection Engines:
  name =oracle1
  type =oracle
  sequence =1
  connect to IP=n.n.n.n
  install dir = /home/oracle18/app/oracle/product/18.0.0.0/dbhome_1
  exec file = /home/oracle18/app/oracle/product/18.0.0.0/dbhome_1/bin/oracle
  db version = 18
  encrypted = no
  port range = 1521 - 1521
  ktap real port = 1521
  identifier = oracle_9.42.29.158(1521,1521,DB_0)
  client = 0.0.0.0/0.0.0.0
  name =mysql2
  type =mysql
  sequence =2
  connect to IP=n.n.n.n
  install dir = /home/mysql57/mysql/data
  exec file = /home/mysql57/mysql/bin/
  encrypted = no
  port range = 3357 - 33060
  ktap real port = 3357
  identifier = mysql_9.42.29.158(3357,33060,DB_2)
  client = 0.0.0.0/0.0.0.0
  name =db23
  type =db2
  sequence =3
  connect to IP=n.n.n.n
  install dir = /home/db2inst1
  exec file = /home/db2inst1/sqllib/adm/db2sysc
  db version = 7
  encrypted = no
  port range = 50000 - 50000
  ktap real port = 50000
  identifier = db2_9.42.29.158(50000,50000,DB_3)
  client = 0.0.0.0/0.0.0.0
```

Related concepts

- [Inspection engine configuration](#)

Related tasks

- [Configuring an inspection engine](#)
- [Configuring an inspection engine](#)

Related reference

- [S-TAP and inspection engine APIs](#)

list_installed_policies

List all of the policies that are installed on the current machine.

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/list_installed_policies
```

GuardAPI syntax

```
list_installed_policies parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

list_managed_units

Run this command on a central manager or a managed unit to output the list all managed units that are managed by the central manager.

This API is available in Guardium v11.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/managed_units
```

GuardAPI syntax

```
list_managed_units parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| unit_type | String | <p>Specify to limit the out to units of the specified type only. Valid values:</p> <ul style="list-style-type: none">• <code>Col</code>• <code>Collector</code>• <code>Agg</code>• <code>Aggregator</code> |
| verbose | Boolean | <p>Valid values:</p> <ul style="list-style-type: none">• <code>0</code> (false): Lists the host names of the systems.• <code>1</code> (true): Lists the host names, IPs, IP mode, versions, whether the system is online, and the central manager or aggregator that the collector reports to (if data is aggregated). <p>Default = <code>0</code> (false)</p> |

Examples

To output a list of collectors only:

```
grdapic list_managed_units unit_type=col verbose=1
Unit Host = server-1, IP=n.n.n.n, type=ManagedCollector, IPMode-IPv4, version=11.4.0_r110686_trunk_1-e179-20210607_1543,online=true
Unit Host = server-2, IP=n.n.n.n, type=ManagedCollector, IPMode-IPv4, version=11.4.0_r110686_trunk_1-e179-20210607_1543,online=true
ok
```

To output a list of all managed units:

```

grdapi list managed_units verbose=1
Unit Host = server-1, IP=n.n.n.n, type=ManagedCollector, IPMode-IPv4, version=11.4.0_r110686_trunk_1-e179-
20210607_1543,online=true
Unit Host = server-2, IP=n.n.n.n, type=ManagedCollector, IPMode-IPv4, version=11.4.0_r110686_trunk_1-e179-
20210607_1543,online=true
Unit Host = server-3, IP=n.n.n.n, type=ManagedAggregator, IPMode-IPv4, version=11.4.0_r110686_trunk_1-e179-
20210607_1543,online=true
ok

```

Related reference

- [Central management APIs](#)

list_members_of_groups_by_desc

This command displays members of one or more groups identified by their group descriptions.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/members_of_groups_by_desc
```

GuardAPI syntax

```
list_members_of_groups_by_desc parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| groups | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> all_managed: execute on all managed units but not the central manager all: execute on all managed units and the central manager group:<group name>: execute on all managed units identified by <group name> host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

list_members_of_groups_by_id

This command displays members of one or more groups identified by their group IDs.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/members_of_groups_by_id
```

GuardAPI syntax

```
list_members_of_groups_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| groupIds | Integer | Required. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

list_oauth_clients

This API lists the API clients that were registered with the `register_oauth_client` API.

This API is available in Guardium V11.2 and later.

GuardAPI syntax

```
list_oauth_clients parameter=value
```

This API takes no parameters.

Related reference

- [register_oauth_client](#)

list_param_mapping_for_function

This command returns the parameter mappings for an API function.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
list_param_mapping_for_function parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| functionName | String | Required. The API name. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapic list_param_mapping_for_function functionName="create_group"
```

Related concepts

- [Mapping APIs to report results](#)

Related reference

- [create_api_parameter_mapping](#)

list_parameter_names_by_report_name

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/list_parameter_names_by_report_name
```

GuardAPI syntax

```
list_parameter_names_by_report_name parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|-------------|
| reportName | String | Required. |

list_policy

This command displays a list of available policies or displays details about a single policy.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/policy
```

GuardAPI syntax

```
list_policy parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| detail | Boolean | Display details about a policy (or all policies if you do not specify a <i>policyDesc</i>). Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| policyDesc | String | The name of one policy to display. If not specified, Guardium returns information about all available policies. |
| verbose | Integer | |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GuardAPI examples

Display details for a specific policy:

```
grdapic list_policy policyDesc="Hadoop Policy"
```

Display a detailed list of available policies:

```
grdapic list_policy
```

Display a list of available policy names (without details):

```
grdapi list_policy detail=false
```

list_policy_fam_rule

This command lists either all the rules, or the specified rule, in a FAM policy.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/famPolicyRule
```

GuardAPI syntax

```
list_policy_fam_rule parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|---|
| policyName | String | Required. Name of FAM policy whose rules are returned in the response. |
| ruleName | String | If no ruleName is entered, all policy rules with details are returned. If a ruleName is entered, details are returned for that rule only. |

Examples

To view all rules in a policy named fam26:

```
list_policy_fam_rule policyName=fam26
```

Related concepts

- [FAM discovery and classification in Windows and UNIX-Linux file servers](#)
- [Using rules for file activity policies](#)

Related reference

- [enable_fam_crawler](#)
- [delete_policy](#)
- [create_policy](#)
- [disable_fam_crawler](#)
- [add_action_to_fam_rule](#)
- [create_fam_rule](#)
- [get_fam_crawler_info](#)
- [policy_fam_rule_delete](#)

list_policy_rules

Display the rules for a specified policy.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/rule
```

GuardAPI syntax

```
list_policy_rules parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-----------------------------------|
| policy | String | Required. The name of the policy. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi list_policy_rules policy="policy1"
```

list_qr_action

This command lists query actions for a specified query definition.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/qr_action
```

GuardAPI syntax

```
list_qr_action parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|---|
| actionName | String | The name of the query rewrite action. |
| definitionName | String | Required. The query rewrite definition name. |
| detail | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • 0: False. Only the name is returned for false • 1: True. List all the associated attributes of the actions. <p>Default = 1 (true)</p> |

Examples

```
grdapi list_qr_action definitionName="case 2"
```

Output:

```
<servername>> grdapi list_qr_action definitionName="case 2"
#####
#####
```

```
QR actions of definition 'case 2' - (id = 1 )
#####
qr action ID: 1
qr action name: qr action2
qr action description: add where by id
```

ok

Example:

```
grdapi list_qr_action definitionName="case 2" detail=false
```

Output:

```
<servername>> grdapi list_qr_action definitionName="case 2" detail=false
#####
QR actions of definition 'case 2' - (id = 1 )
#####
qr action2
ok
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

list_qr_add_where

Lists "add where" functions for a specified query action and query definition pair.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/qr_add_where
```

GuardAPI syntax

```
list_qr_add_where parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|---|
| actionName | String | Required. The name of the query rewrite action. |
| definitionName | String | Required. The query rewrite definition name. |

Examples

Say something about the example

```
grdapi list_qr_add_where actionName="qrw_act_addwhere_id2" definitionName="qrw_def_Oracle_1"
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

list_qr_add_where_by_id

This command lists "add where" functions for a specified query action.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/list_qr_add_where_by_id
```

GuardAPI syntax

```
list_qr_add_where_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|---|
| qrActionId | Long | Required. The unique identifier for the query rewrite action. |

Examples

```
grdapi list_qr_add_where_by_id qrActionId=20023
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

list_qr_condition

Lists the query rewrite conditions that are associated with a particular query rewrite definition.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/qr_condition
```

GuardAPI syntax

```
list_qr_condition parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|---|
| conditionName | String | The name of a query rewrite condition. |
| definitionName | String | Required. A query rewrite definition. |
| detail | Boolean | Valid values: <ul style="list-style-type: none">• 0: False. Returns the name only.• 1: True. Returns all the associated attributes of the conditions. Default = 1 (true) |

Examples

```
grdapi list_qr_condition definitionName="case 2" conditionName="qr cond2"
```

Output:

```
<servername>> grdapi list_qr_condition definitionName="case 2" conditionName="qr cond2"
#####
QR Conditions of Definition 'case 2' - (id = 1 )
#####

qr condition id: 1
qr condition name: qr cond2
qr definition ID: 1
qr condition verb: *
qr condition object: *
qr condition dept: -1
is verb regex: false
is object regex: false
is action for all rule verbs: false
is action for all rule objects: false
qr condition order: 1
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

list_qr_condition_to_action

This command lists the associations between a query rewrite condition and a query rewrite action for a particular query definition.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/qr_condition_to_action
```

GuardAPI syntax

```
list_qr_condition_to_action parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|---|
| actionName | String | Required. The unique identifier for the query rewrite action. |
| definitionName | String | Required. A query rewrite definition. |
| detail | Boolean | Valid values: <ul style="list-style-type: none">• 0: False. Returns the name only.• 1: True. Returns all the associated attributes of the conditions. Default = 1 (true) |

Examples

```
grdapi list_qr_condition_to_action actionName="qr action15_2" definitionName="case 15"
```

Output:

```
<servername>> grdapi list_qr_condition_to_action actionName="qr action2" definitionName="case 2"
#####
QR Conditions of Action 'qr action2' - (id = 1 )
#####

qr condition id: 1
qr condition name: qr cond2
qr definition ID: 1
qr condition verb: *
qr condition object: *
qr condition dept: -1
is verb regex: false
is object regex: false
is action for all rule verbs: false
is action for all rule objects: false
qr condition order: 1
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

list_qr_definitions

This command outputs query rewrite definitions.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/list_qr_definitions
```

GuardAPI syntax

```
list_qr_definitions parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|-----------------------------|
| definitionName | String | A query rewrite definition. |

| Parameter | Value type | Description |
|-----------|------------|--|
| detail | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • 0: False. Returns the name only. • 1: True. Returns all the associated attributes of the conditions. <p>Default = 1 (true)</p> |

Examples

```
grdapi list_qr_definitions

Output:

<servername>> grdapi list_qr_definitions
#####
QR Definitions
#####
qr definition ID: 1
qr definition name: case 2
qr definition description:
is negation set on qr conditions: false
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

list_qr_replace_element

This command outputs replacements for a specified query rewrite action and query rewrite definition pair.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/qr_replace_element
```

GuardAPI syntax

```
list_qr_replace_element parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|--|
| actionName | String | Required. A query rewrite action. |
| definitionName | String | Required. A query rewrite definition. |
| detail | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • 0: False. Returns the name only. • 1: True. Returns all the associated attributes of the conditions. <p>Default = 1 (true)</p> |
| replaceType | String | <p>Valid values:</p> <ul style="list-style-type: none"> • SELECT • VERB • OBJECT • SENTENCE • SELECTLIST |

Examples

```
grdapi list_qr_replace_element actionName="qr action2" definitionName="case 2"
```

Output:

```
<servername>> grdapi list_qr_replace_element actionName="qr action2" definitionName="case 2"
#####
QR replace elements for action 'qr action2' - (qrActionId = 1 )
```

```
#####
qr replace element ID: 1
qr replace type: object
qr replace from: emp
qr replace to: NEW_EMP
qr is from regex: false
qr is from all rule elements: false

*****
qr replace element ID: 2
qr replace type: selectList
qr replace from: Whole select list
qr replace to: EMPNO,SAL
qr is from regex: false
qr is from all rule elements: false
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

list_qr_replace_elementById

This command outputs replacements for a specified query rewrite action.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/list_qr_replace_elementById
```

GuardAPI syntax

```
list_qr_replace_elementById parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|--|
| detail | Boolean | Valid values: <ul style="list-style-type: none"> • 0 (false) • 1 (true) Default = 1 |
| qrActionId | Long | Required. The unique identifier for the query rewrite action. |
| replaceType | String | Valid values: <ul style="list-style-type: none"> • SELECT • VERB • OBJECT • SENTENCE • SELECTLIST |

Examples

```
grdapic list_qr_replace_elementById detail=true qrActionId="22222" replaceType="OBJECT"
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

list_quick_search_groups

This command returns a list of groups defined for quick search.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
list_quick_search_groups parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To output the quick search groups:

```
grdapi list_quick_search_groups
```

Related concepts

- [Investigation dashboard](#)

Related reference

- [Investigation dashboard APIs](#)

list_ranger_configs

This command lists all Ranger configurations on the specified Guardium host(s). The result is shown as the administrator account, the host and port, and the cluster name.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/list_ranger_configs
```

GuardAPI syntax

```
list_ranger_configs parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GrdAPI Example

List the current Ranger configuration (cluster) defined on this Guardium appliance:

```
grdapi list_ranger_configs
```

Sample output:

```
ID=0  
admin@<server>:8080 Cluster4
```

REST API Example

List the current Ranger configuration (cluster) defined on this Guardium appliance.

```
curl -k -i --header "Authorization:Bearer <access token>" https://<Guardium host name>:8443/restAPI/list_ranger_configs
```

Sample output when there is no configuration:

```
HTTP/1.1 200 OK  
X-FRAME-OPTIONS: SAMEORIGIN  
Set-Cookie: JSESSIONID=8B9581F4DA85E980DBD4C152CB8AD975; Path=/; Secure; HttpOnly  
Cache-Control: max-age=86400  
Expires: Tue, 20 Sep 2016 21:32:09 GMT  
Access-Control-Allow-Methods: POST, GET, PUT, DELETE  
Access-Control-Allow-Headers: authorization, origin, X-Requested-With, Content-Type, AcceptAccess-Control-Max-Age: 18000  
Content-Type: application/json;charset=UTF-8Content-Length: 62Date: Mon, 19 Sep 2016 21:32:09 GMTServer: SQL Guard
```

Sample output with all services configured:

```
[  
  {  
    "id": 1,  
    "clusterName": "Cluster4",  
    "serverHost": "<server>",  
    "serverPort": 8080,  
    "userName": "admin",  
    "password": "nnnnnn",  
    "lastRefresh": "2016-09-14 13:45:10",  
    "status": [  
      {  
        "id": 1,  
        "ambariConfigId": 1,  
        "service": {  
          "id": 1,  
          "label": "HBase",  
          "value": "HBASE"  
        },  
        "stapHost": {  
          "id": 22,  
          "name": "<server>",  
          "value": "<server>",  
          "port": "5555",  
          "stapStatus": 2  
        },  
        "isMonitored": true,  
        "port": "5555",  
        "editMode": true  
      },  
      {  
        "id": 2,  
        "ambariConfigId": 1,  
        "service": {  
          "id": 2,  
          "label": "HDFS",  
          "value": "HDFS"  
        },  
        "stapHost": {  
          "id": 22,  
          "name": "<server>",  
          "value": "<server>",  
          "port": "5555",  
          "stapStatus": 2  
        },  
        "isMonitored": false,  
        "port": "5555",  
        "editMode": true  
      },  
      {  
        "id": 3,  
        "ambariConfigId": 1,  
        "service": {  
          "id": 3,  
          "label": "Hive",  
          "value": "HIVE"  
        },  
        "stapHost": {  
          "id": 28,  
          "name": "<server>",  
          "value": "<server>",  
          "port": "5534",  
          "stapStatus": 2  
        },  
        "isMonitored": false,  
        "port": "5534",  
        "editMode": true  
      }  
    ]  
]
```

```

        "isMonitored": true,
        "port": "5534",
        "editMode": true
    },
    {
        "id": 4,
        "ambariConfigId": 1,
        "service": {
            "id": 4,
            "label": "Kafka",
            "value": "KAFKA"
        },
        "stapHost": {
            "id": 22,
            "name": "<server>",
            "value": "<server>",
            "port": "5555",
            "stapStatus": 2
        },
        "isMonitored": true,
        "port": "5555",
        "editMode": true
    },
    {
        "id": 5,
        "ambariConfigId": 1,
        "service": {
            "id": 5,
            "label": "Storm",
            "value": "STORM"
        },
        "stapHost": {
            "id": 22,
            "name": "<server>",
            "value": "<server>",
            "port": "5555",
            "stapStatus": 2
        },
        "isMonitored": false,
        "port": "5555",
        "editMode": true
    }
]

```

Related concepts

- [Hadoop integration using Hortonworks and Apache Ranger](#)

Related reference

- [Hadoop monitoring APIs](#)
- [S-TAP Hadoop parameters](#)

list_ranger_hdfs_config

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/list_ranger_hdfs_config
```

GuardAPI syntax

```
list_ranger_hdfs_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

list_ranger_staps

This command lists all S-TAPs that are eligible for Ranger configuration or are currently configured for Ranger integration. (All S-TAPs that are not configured for Kafka (Cloudera integration).)

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/list_ranger_staps
```

GuardAPI syntax

```
list_ranger_staps parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GrdAPI example

To find databases that host Ranger-configured S-TAPs that report to this Guardium® system:

```
grdapic list_ranger_staps
```

System output:

```
ID=0
<DB server name>:5556
<DB server name>:5555
```

REST API example

To find databases that host Ranger-configured S-TAPs that report to the specified Guardium system:

```
curl -k -i --headere-492d-b3ef-23d1b073eb05" https://<Guardium server name>:8443/restAPI/list_ranger_staps
```

System output, which only displays S-TAPs with `stapStatus=2`, meaning the S-TAP® is active and properly synchronized:

```
[
{
"id": 18,
"name": "<DB server>",
"value": "<DB server>",
"port": "5534",
"stapStatus": 2
},
```

```
{
  "id": 24,
  "name": "<DB server>",
  "value": "<DB server>",
  "port": "5534",
  "stapStatus": 2
},
{
  "id": 25,
  "name": "<DB server>",
  "value": "<DB server>",
  "port": "5555",
  "stapStatus": 2
}
```

Related concepts

- [Hadoop integration using Hortonworks and Apache Ranger](#)

Related reference

- [Hadoop monitoring APIs](#)
- [S-TAP Hadoop parameters](#)

list_ready_files

This API is available in Guardium V10.1.4 and later.

GuardAPI syntax

```
list_ready_files parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> all_managed: execute on all managed units but not the central manager all: execute on all managed units and the central manager group:<group name>: execute on all managed units identified by <group name> host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

list_roles

This command lists the roles available on your Guardium system.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/role
```

GuardAPI syntax

```
list_roles
```

This API takes no parameters.

Gaurd API example

```
grdapic list_roles
```

Related concepts

- [Understanding roles](#)

list_roles_granted_to_object_by_Name

This command returns the roles that are assigned, by name, to a specified object, such as a Classification process.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/role
```

GuardAPI syntax

```
list_roles_granted_to_object_by_Name parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| objectName | String | Required. The name of the object for which to list the roles. |
| objectType | String | Required. The name of the object type. For valid values, call <code>list_roles_granted_to_object_by_Name</code> from the command line with <code>--help=true</code> . |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group: <group name>; execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi list_roles_granted_to_object_by_Name objectType=PrivacySet objectName="privacySet 1"
```

list_roles_granted_to_object_by_id

This command returns the roles that are assigned, by ID, to a specified object, such as a Classification process.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/roles_granted_to_object_by_id
```

GuardAPI syntax

```
list_roles_granted_to_object_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------|------------|---|
| objectId | Integer | Required. The ID of the object for which to list the roles. |
| objectTypeId | Integer | Required. The ID of the object type. For valid values, call <code>list_roles_granted_to_object_by_id</code> from the command line with <code>--help=true</code> . |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi list_roles_granted_to_object_by_id objectTypeId=7 objectId=1
```

list_rules_with_threshold

Run this command to see which rules have thresholds (that trigger opening an active threat analytics case).

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/list_rules_thresholds
```

GuardAPI syntax

```
list_rules_with_threshold parameter=value
```

This API does not take any parameters.

Examples

To output a list of rules with thresholds, and their policies:

```
grdapi list_rules_with_thresholds
```

Sample output

```
grdapi list_rules_with_threshold
ID=0
Rule Name: "Failed Login - GDPR Personal Data -Alert if repeated", Policy Name: Rule1, Threshold: 3
Rule Name: NP, Policy Name: Rule3, Threshold: 5
```

Related tasks

- [Creating and installing a policy and policy rules](#)
- [Creating threat categories from policy rules](#)

Related reference

- [Policy and rule APIs](#)
- [Active threat analytics and risk spotter APIs](#)

list_running_processes

This API lists long-running processes that are running on the current Guardium system.

In some cases, processes continue to run past the time specified by the Report/Monitor Query Timeout setting (in [Manage > Maintenance > General > Running Query Monitor](#)). Use `list_running_processes` to find the process ID of any processes that run past the timeout. You can then stop the processes with the [kill_running_process](#) API.

You can also view or change the value of the Report/Monitor Query Timeout by using the [show_maximum_query_duration](#) and [store_maximum_query_duration](#) APIs.

The `list_running_processes` API takes no parameters.

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/list_running_processes
```

GuardAPI syntax

```
list_running_processes
```

Examples

```
grdapi list_running_processes
```

Related concepts

- [Running Query Monitor](#)

Related reference

- [kill_running_process](#)
- [show_maximum_query_duration](#)
- [store_maximum_query_duration](#)

list_scheduler_jobs

Run this command to see all schedules jobs.

This API is available in Guardium V10.1.4 and later.

GuardAPI syntax

```
list_scheduler_jobs parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapi list_scheduler_jobs
ID=0
##### EXTENDED SCHEDULER JOB INFO0 #####
TRIGGER_NAME=userSynchronizationTrigger
TRIGGER_GROUP=userSynchronizationJobGroup
JOB_NAME=userSynchronizationJob
GROUP_NAME=userSynchronizationJobGroup
JOB_CATEGORY=userSynchronization
JOB_STATE=SCHEDULED
JOB_NEXT_FIRE_TIME=Mon Jul 27 09:30:00 EDT 2020
JOB_PREV_FIRE_TIME=Mon Jul 27 09:00:00 EDT 2020
JOB_ASSOCIATED_OBJECT_TYPE=job.type.userSynchronization
JOB_ASSOCIATED_OBJECT=userSynchronization
JOB_ASSOCIATED_OBJECT_ID=-1
JOB_LAST_EXECUTION_STATE=SUCCESS

##### EXTENDED SCHEDULER JOB INFO1 #####
TRIGGER_NAME=ConnectivityMonitor
TRIGGER_GROUP=ConnectivityMonitor
JOB_NAME=ConnectivityMonitor
GROUP_NAME=ConnectivityMonitor
JOB_CATEGORY=connectivityMonitor
JOB_STATE=SCHEDULED
```

```

JOB_NEXT_FIRE_TIME=Mon Jul 27 09:15:00 EDT 2020
JOB_PREV_FIRE_TIME=Mon Jul 27 09:12:00 EDT 2020
JOB_ASSOCIATED_OBJECT_TYPE=job.type.ConnectivityMonitor
JOB_ASSOCIATED_OBJECT=connectivityMonitor
JOB_ASSOCIATED_OBJECT_ID=-1
JOB_LAST_EXECUTION_STATE=SUCCESS

##### EXTENDED SCHEDULER JOB INFO2 #####
TRIGGER_NAME=purgeJobTrigger
TRIGGER_GROUP=purgeJobGroup
JOB_NAME=purgeJob
GROUP_NAME=purgeJobGroup
JOB_CATEGORY=purgeJob
JOB_STATE=SCHEDULED
JOB_NEXT_FIRE_TIME=Tue Jul 28 00:05:00 EDT 2020
JOB_PREV_FIRE_TIME=Mon Jul 27 00:05:00 EDT 2020
JOB_ASSOCIATED_OBJECT_TYPE=job.type.purgeJob
JOB_ASSOCIATED_OBJECT=purgeJob
JOB_ASSOCIATED_OBJECT_ID=-1
JOB_LAST_EXECUTION_STATE=SUCCESS

##### EXTENDED SCHEDULER JOB INFO3 #####
TRIGGER_NAME=dataArchiveTrigger
TRIGGER_GROUP=dataIOJobGroup
JOB_NAME=dataArchiveJob
GROUP_NAME=dataIOJobGroup
JOB_CATEGORY=DataArchive
JOB_STATE=SCHEDULED
JOB_NEXT_FIRE_TIME=Tue Jul 28 05:00:00 EDT 2020
JOB_PREV_FIRE_TIME=Mon Jul 27 05:00:00 EDT 2020
JOB_ASSOCIATED_OBJECT_TYPE=job.type.DataArchive
JOB_ASSOCIATED_OBJECT=DataArchive
JOB_ASSOCIATED_OBJECT_ID=-1
JOB_LAST_EXECUTION_STATE=SUCCESS

##### EXTENDED SCHEDULER JOB INFO4 #####
TRIGGER_NAME=updateStapChangeTrigger
TRIGGER_GROUP=updateStapChangeJobGroup
JOB_NAME=updateStapChangeJob
GROUP_NAME=updateStapChangeJobGroup
JOB_CATEGORY=updateStapChange
JOB_STATE=SCHEDULED
JOB_NEXT_FIRE_TIME=Mon Jul 27 09:15:00 EDT 2020
JOB_PREV_FIRE_TIME=Mon Jul 27 09:10:00 EDT 2020
JOB_ASSOCIATED_OBJECT_TYPE=job.type.updateStapChange
JOB_ASSOCIATED_OBJECT=updateStapChange
JOB_ASSOCIATED_OBJECT_ID=-1
JOB_LAST_EXECUTION_STATE=SUCCESS

##### EXTENDED SCHEDULER JOB INFO5 #####
TRIGGER_NAME=updateToDoTrigger
TRIGGER_GROUP=updateToDoJobGroup
JOB_NAME=updateToDoJob
GROUP_NAME=updateToDoJobGroup
JOB_CATEGORY=updateToDo
JOB_STATE=SCHEDULED
JOB_NEXT_FIRE_TIME=Mon Jul 27 09:20:00 EDT 2020
JOB_PREV_FIRE_TIME=Mon Jul 27 09:10:00 EDT 2020
JOB_ASSOCIATED_OBJECT_TYPE=job.type.updateToDo
JOB_ASSOCIATED_OBJECT=updateToDo
JOB_ASSOCIATED_OBJECT_ID=-1
JOB_LAST_EXECUTION_STATE=SUCCESS

##### EXTENDED SCHEDULER JOB INFO6 #####
TRIGGER_NAME=stapF5CorrelationTrigger
TRIGGER_GROUP=stapF5CorrelationJobGroup
JOB_NAME=stapF5CorrelationJob
GROUP_NAME=stapF5CorrelationJobGroup
JOB_CATEGORY=stapF5Correlation
JOB_STATE=SCHEDULED
JOB_NEXT_FIRE_TIME=Mon Jul 27 09:30:00 EDT 2020
JOB_PREV_FIRE_TIME=Mon Jul 27 09:00:00 EDT 2020
JOB_ASSOCIATED_OBJECT_TYPE=job.type.stapF5Correlation
JOB_ASSOCIATED_OBJECT=stapF5Correlation
JOB_ASSOCIATED_OBJECT_ID=-1
JOB_LAST_EXECUTION_STATE=SUCCESS

##### EXTENDED SCHEDULER JOB INFO7 #####
##### EXTENDED SCHEDULER JOB INFO8 #####
TRIGGER_NAME=DataMartExtractionJobTrigger_51
TRIGGER_GROUP=DataMartExtractionJobGroup
JOB_NAME=DataMartExtractionJob_51
GROUP_NAME=DataMartExtractionJobGroup
JOB_CATEGORY=dataMartExtraction
JOB_STATE=SCHEDULED
JOB_NEXT_FIRE_TIME=Mon Jul 27 10:00:00 EDT 2020
JOB_PREV_FIRE_TIME=Mon Jul 27 09:00:00 EDT 2020
JOB_ASSOCIATED_OBJECT_TYPE=job.type.dataMartExtraction
JOB_ASSOCIATED_OBJECT=Lucene VA Results
JOB_ASSOCIATED_OBJECT_ID=51
JOB_LAST_EXECUTION_STATE=SUCCESS

grdapi list_scheduler_jobs
ID=0
##### EXTENDED SCHEDULER JOB INFO9 #####
TRIGGER_NAME=userSynchronizationTrigger

```

```

TRIGGER_GROUP=userSynchronizationJobGroup
JOB_NAME=userSynchronizationJob
GROUP_NAME=userSynchronizationJobGroup
JOB_CATEGORY=userSynchronization
JOB_STATE=SCHEDULED
JOB_NEXT_FIRE_TIME=Mon Jul 27 09:30:00 EDT 2020
JOB_PREV_FIRE_TIME=Mon Jul 27 09:00:00 EDT 2020
JOB_ASSOCIATED_OBJECT_TYPE=job.type.userSynchronization
JOB_ASSOCIATED_OBJECT=userSynchronization
JOB_ASSOCIATED_OBJECT_ID=-1
JOB_LAST_EXECUTION_STATE=SUCCESS

```

Related concepts

- [Scheduling](#)
- [Job dependencies](#)

Related reference

- [Schedule and job dependencies APIs](#)

list_schedules

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/schedules
```

GuardAPI syntax

```
list_schedules parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| jobName | String | |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> all_managed: execute on all managed units but not the central manager all: execute on all managed units and the central manager group:<group name>: execute on all managed units identified by <group name> host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

list_stap_verification_results

This API returns the details and the verification results for each S-TAP® that reports to the specified Guardium® system.

This GuardAPI is available in Guardium V9.5 and later.

The REST API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/list_stap_verification_results
```

GuardAPI syntax

```
list_stap_verification_results parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| stapHost | String | |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To return the verification status of the S-TAPs reporting to this Guardium system

```
grdapi list_stap_verification_results
S-TAP Host = 9.42.29.158
Protocol = oracle
Port Range = 1521-1521
Inspection Engine Identifier = oracle_9.42.29.158(1521,1521,DB_0)
Verification Status = Unverified

S-TAP Host = 9.42.29.158
Protocol = mysql
Port Range = 3357-33060
Inspection Engine Identifier = mysql_9.42.29.158(3357,33060,DB_2)
Verification Status = Unverified

S-TAP Host = 9.42.29.158
Protocol = db2
Port Range = 50000-50000
Inspection Engine Identifier = db2_9.42.29.158(50000,50000,DB_3)
Verification Status = Unverified
```

Related concepts

- [Windows: inspection engine verification](#)
- [Linux-UNIX: inspection engine verification](#)

list_staps

This API returns a list of database servers that host S-TAPs that report to the specified Guardium® system, both as primary and secondary host. Optionally, return only the databases having S-TAPs for which the specified Guardium system is the active host.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/stap
```

GuardAPI syntax

```
list_staps parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|---|
| onlyActive | Boolean | <p>Valid values:</p> <ul style="list-style-type: none">• 0: list all hosts whose S-TAPs are configured to use this Guardium system as either a primary or secondary host.• 1: list only those hosts having S-TAPs for which this Guardium system is the active host. <p>Default = 1 (true)</p> |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To find databases that host S-TAPs that report to this Guardium system, as both the primary and secondary host:

```
grdapi list_staps onlyActive=false
```

This command provides the following output:

```
staps:
stap host = 144.129.31.33
stap host = 144.129.31.17
stap host = 144.129.31.248
ok
```

Related reference

- [S-TAP and inspection engine APIs](#)

list_test_detail_exception

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/test_detail_exception
```

GuardAPI syntax

```
list_test_detail_exception parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------------|------------|---|
| approver | String | |
| assessmentDesc | String | |
| assessmentScope | String | |
| datasourceGroup | String | |
| datasourceName | String | |
| datasourceScope | String | |
| datasourceType | String | |
| detailExceptionValue | String | |
| displayLimit | Integer | |
| exceptionType | String | Valid values: <ul style="list-style-type: none"> • <code>text</code> • <code>regex</code> • <code>0</code> • <code>1</code> |
| testDescription | String | |
| validDate | String | |

list_test_exception

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/test_exception
```

GuardAPI syntax

```
list_test_exception parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| approver | String | |
| assessmentDesc | String | |
| assessmentScope | String | Valid values: <ul style="list-style-type: none">• CURRENT• ALL• 0• 1 |
| datasourceGroup | String | |
| datasourceName | String | |
| datasourceScope | String | Valid values: <ul style="list-style-type: none">• SINGLE• GROUP• ALL• 0• 1• 2 |
| datasourceType | String | For valid values, call <code>list_test_exception</code> from the command line with <code>--help=true</code> . |
| displayLimit | Integer | |
| explanation | String | |
| testDescription | String | |
| validDate | String | |

list_test_exception_by_id

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/test_exception
```

GuardAPI syntax

```
list_test_exception_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|-------------|
| testExceptionId | Long | Required. |

list_user_hierarchy_by_parent_user

This command returns the user hierarchy for a specified parent user.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/user_hierarchy
```

GuardAPI syntax

```
list_user_hierarchy_by_parent_user parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| create | String | Valid values: <ul style="list-style-type: none">• <i>true</i>• <i>false</i> When set to true, returns the value of the users in the format of a create_user_hierarchy statement. |
| userName | String | The name of the parent user. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GuardAPI examples

In the following examples, George and Harry are both children of AdminManager.

```
grdapi list_user_hierarchy_by_parent_user userName=Fred
```

Sample output

```
ID=0
Name: George  Id =      1, Parent =    20000, Child =    20001, Type: user
Name: Harry   Id =      3, Parent =    20000, Child =    20002, Type: user
ok
```

The same command, but with `create=true`:

```
grdapi list_user_hierarchy_by_parent_user userName=AdminManager create=true
```

Sample output

```
ID=0
grdapi create_user_hierarchy userName="George" parentUserName="AdminManager"
grdapi create_user_hierarchy userName="Harry" parentUserName="AdminManager"
ok
```

Related concepts

- [Data Security - User Hierarchy and Database Associations](#)

Related reference

- [create_user_hierarchy](#)

list_user_roles

This API lists all the roles associated with a specified user.

To find a user name, use the [list_users](#) API. To change the roles for a user, use the [set_user_roles](#) API. To make other changes to a user's account, use the [update_user](#) API.

Note: You must have appropriate permissions to user the `set_user_roles` and `update_user` APIs.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/userRole
```

GuardAPI syntax

```
list_user_roles parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---------------------------------|
| userName | String | Required. The name of the user. |

Examples

To list the roles for user Fred McDerm:

```
grdapi list_user_roles userName="Fred McDerm"
```

Sample output:

```
ID=20001
Roles of User: Fred McDerm
admin
dba
diag
cli
ok
```

list_users

This API returns a list of Guardium users and account information.

The **list_users** API requires that the CLI account issuing the command is associated with a GUI account that has the *accessmgr* and *cli* roles. Associate CLI and GUI accounts using the **set guimuser** CLI command. For more information, see [User account, password, and authentication CLI Commands](#).

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/user
```

GuardAPI syntax

```
list_users
```

Examples

This command returns a list of all users on this system. For example:

```
grdapi list_users
```

Returns the following information:

```
##### User 3 #####
Username: Fred McDerm
First Name: Fred
Last Name: McDerm
Email: fredmcd@company.com
Disabled: false
Password changed: 2023-08-15 11:26:20
Password expires: 2023-11-13 11:26:20
#####
User 1 #####
Username: joan.darcy
First Name: Joan
Last Name: Darcy
Email: joan.darcy@company.com
Disabled: false
Password changed: 2023-08-02 10:00:00
Password expires: 2023-11-01 10:00:00
#####
User 20 #####
Username: hadrian.s.wall
First Name: Hadrian
Last Name: Wall
Email: hadrian.s.wall@company.com
Disabled: true
Password changed: 2023-05-12 11:56:00
Password expires: 2023-08-10 11:56:00
ok
```

Related reference

- [create_user](#)

- [update_user](#)

list_utilization_thresholds

This API is available in Guardium V9.5 and later.

This API takes no parameters.

GuardAPI syntax

```
list_utilization_thresholds
```

load_all_packages

This API loads universal connector packages to the specified path.

This API is available in Guardium v12.0 and later.

GuardAPI syntax

```
load_all_packages parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| path | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

load_mongodb

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
load_mongodb parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|-------------|
| collectionName | String | Required. |
| database | String | Required. |
| host | String | Required. |
| password | String | Required. |
| port | Integer | Required. |
| user | String | Required. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

load_mongodb_by_datasource

This API is available in Guardium V10.1.4 and later.

GuardAPI syntax

```
load_mongodb_by_datasource parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| collectionName | String | Required. |
| datasourceName | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

local_disable_big_data_intelligence

Run this command on a managed unit to disable it (or the specified unit) from sending data to the active profile.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/local_disable_big_data_intelligence
```

GuardAPI syntax

```
local_disable_big_data_intelligence parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To stop the managed unit from sending data to the active profile:

```
local_disable_big_data_intelligence
```

Related concepts

- [Big Data Intelligence with data marts](#)

Related reference

- [Big Data Intelligence APIs](#)

local_enable_big_data_interface

Run this command on a collector that was offline or not in the MU group when the profile was activated; or on a collector that is not in the MU group, to add its data included the the extraction defined by the profile. Advanced users can use this command for extracting data from collectors that use a different profile.

For example, two managed units of a central manager run only VA, and the other managed units are tracking other data. You would create a second profile that is a subset of the main profile, and run it only on the specified units. However, the local profile does not have a target for the data; add it using the command:
`datamart_update_copy_file_info`.

This API is available in Guardium V10.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/bigDataInterface
```

GuardAPI syntax

```
local_enable_big_data_interface parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| profile_name | String | Required. An existing profile. For valid values, run <code>grdapi get_extraction_profile_info</code> or call <code>local_enable_big_data_interface</code> from the command line with <code>--help=true</code> . |
| start_date | Date | When to start sending data to the Big Data datasource. Default = time at which the command is executed. Format is either <code>NOW - <n> <minute hour day week month; or yyyy-mm-dd hh:mm:ss</code> |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To add the managed units adata to the profile sql_all:

```
local_enable_big_data_interface profile_name=sql_all
```

Related concepts

- [Big Data Intelligence with data marts](#)

Related reference

- [Big Data Intelligence APIs](#)

make_bundle_with_uploaded_kernel_module

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
make_bundle_with_uploaded_kernel_module parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

make_primary_cm

Run this API on the backup (secondary) central manager to change it to the primary central manager.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/make_primary_cm
```

GuardAPI syntax

```
make_primary_cm
```

This API takes no parameters.

Examples

Enter this command on the secondary central manager to change it to the primary central manager:

```
grdapic make_primary_cm
```

Related concepts

- [Central manager redundancy](#)

Related reference

- [Central management APIs](#)

migrate_stap_config

This command configures and moves one or more S-TAPs to Guardium® Insights.

Before you can migrate the S-TAPs, you must push Guardium Insights certificate chain (either from the Guardium Data Protection GUI or by using the [push_insights_trust](#) API).

If the migrate_stap_config command is successful, the S-TAP® is removed from Guardium Data Protection.

Notes:

- Guardium Insights 3.1 or later is required.
- You can migrate only UNIX S-TAPs.

This API is available in Guardium v11.4 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/stap_config
```

GuardAPI syntax

```
migrate_stap_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| routeName | String | Required. The DNS hostname for the Guardium Insights deployment. The DNS hostname is the same as the URL for the UI (without the https:// prefix). |
| stapHost | String | Required. Specify the name of one or more S-TAP hosts (separated by a comma), or specify <i>all_unix_active</i> . For valid values, call migrate_stap_config from the command line with --help=true. |
| tenantId | String | Required. The Guardium Insights tenant ID, including the <i>TNT_</i> prefix. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• <i>all_managed</i>: Run on all managed units but not the central manager• <i>group:<group name></i>: Run on all managed units identified by <group name>• host name or IP address of a managed unit: Specified from the central manager to execute on a managed unit. For example, <i>api_target_host=10.0.1.123</i>. Note: IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Example

```
vm150.mycompany.com> grdapic migrate_stap_config stapHost=rh6u9x64t.mycompany.com api_target_host=sys-vm154.mycompany.com
routeName=sys.tokyo-0a94651246c65639d6ebe7da606c1234-0000.ca-tor.containers.appdomain.cloud tenantId=TNT_DARBESKTVGTGYAMF7RABCD
ID=0
sys-vm154.isslab.usga.ibm.com
ID=0
Insights data sent to active synchronized S-TAP hosts:
rh6u9x64t.mycompany.com
```

Related reference

- [push_insights_trust](#)

Related information

- [Linux-UNIX: Configuring S-TAP in the S-TAP Control page](#)

modify_autodetect_process

Use this command to modify an auto-discovery process.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/autodetect_processes
```

GuardAPI syntax

```
modify_autodetect_process parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------------|------------|---|
| check_ICMP_echo | Boolean | Whether or not Nmap sends an ICMP echo request. PE parameter to nmap. This is an nmap parameter. nmap options are configurable only by API (not by GUI). For details of nmap parameters and their impact on scan performance, see man nmap. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| host_timeout | Integer | Timeout value, in seconds, for determining how long Guardium waits for a probe response before giving up or retransmitting the probe. This is an nmap parameter. nmap options are configurable only by API (not by GUI). For details of nmap parameters and their impact on scan performance, see man nmap. |
| process_name | String | Required. Name of the auto-discovery process |
| run_probe_after_scan | Boolean | Determines whether or not to run a probe job immediately after the scan job completes. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| use_dns | String | This is an nmap parameter. nmap options are configurable only by API (not by GUI). For details of nmap parameters and their impact on scan performance, see man nmap. Valid values: <ul style="list-style-type: none">• true: always• false: never• n: never• R: always |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To change the configuration of the process myProcess to run the probe after the scan completes, enter:

```
grdapi create_autodetect_process process_name=myProcess run_probe_after_scan=true
```

Related concepts

- [Database auto-discovery](#)

Related reference

- [Auto-discovery APIs](#)

modify_ef_mapping

This command modifies the table or column names used for an external feed mapping.

Sometimes the names generated by `create_ef_mapping` are not suitable for a particular database, and `modify_ef_mapping` can be used to adjust the names to fit database requirements. To protect predefined Guardium mappings, only mappings with an identification key greater than 20000 can be modified.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/modify_ef_mapping
```

GuardAPI syntax

```
modify_ef_mapping parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| modifyObj | String | Required. Specifies the database object to modify. Use the list_ef_mapping command to see the table and column names for a mapping.
Valid values: <ul style="list-style-type: none">• <i>table</i>• <i>column</i> |
| newName | String | Required. The new table or column name to use. |
| oldName | String | Required. The table or column name to modify. |
| reportName | String | Required. Name of the report mapping to modify. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

Use this command to change the table name from *SESSIONS_PER_DAY* to *SESSIONS-PER-DAY* in the Sessions per Day report mapping:

```
grdapi modify_ef_mapping reportName="Sessions per Day" modifyObj=table oldName=SESSIONS_PER_DAY newName=SESSIONS-PER-DAY
```

modify_ef_sql_mode

Enables (or disables) an external feed report to run with dynamic SQL.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/modify_ef_sql_mode
```

GuardAPI syntax

```
modify_ef_sql_mode parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------|------------|---|
| reportName | String | Required. The name of a custom report for which you want to enable dynamic SQL. |
| useDynamicSQL | String | Required. Toggles the ability to use dynamic SQL on or off. Valid values: <ul style="list-style-type: none">• <i>yes</i>• <i>no</i>• <i>true</i>• <i>false</i> |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Example

```
>grdapi modify_ef_sql_mode reportName="Test_API_Exception" useDynamicSQL=true
```

modify_guard_param

This generic API updates the values of specific parameters for various Guardium functions.

Functions that use this parameter include:

- [Alerting.parameters](#)
- [Analyze limits parameters](#)
- [Classification parameters](#)
- [CyberArk parameters](#)
- [Data mart parameters](#)
- [Datasource parameters](#)
- [Health analyzer parameters](#)
- [Inspection engine parameters](#)
- [Manage_SQL parameters](#)
- [Nanny parameters](#)
- [Offline help parameters](#)
- [Quartz scheduler parameters](#)
- [Smart card parameters](#)
- [Sniffer parameters](#)
- [SNMP parameters](#)
- [Syslog TCP parameters](#)
- [Threat analytics parameters](#)
- [Vulnerability Assessment parameters](#)
- [Other parameters](#)

Note: Use [get_all_modifiable_guard_params](#) to display a list of the parameters that can be modified with this API.

This API is available in Guardium V10.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/modify_guard_param
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| paramName | String | Required. One of the parameters that are described in the following sections. |
| paramValue | String | The new value for the parameter. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Alerting parameters

| Parameter | Value Type | Description |
|------------------------|------------|---|
| ALERT_VERB_NUM_LIMIT | Integer | Sets the maximum number of SQL verbs to show in the Alert log. Valid value is a positive integer between 1 and 50. The default is 10. |
| ANTLR3_REMOVE_COMMENTS | Boolean | Enables or disables logging of comments.
Valid values: <ul style="list-style-type: none">• 0: logging of comments is enabled• 1: logging of comments is disabled Default = 0 |
| SMTP_TIMEOUT | Integer | Alerter SMTP Time-Out. |
| STARTTLS | String | Sets TLS data encryption for the alerter email server.
Valid values: <ul style="list-style-type: none">• <i>TLS</i>: Use TLS data encryption.• <i>SSL</i>: Use TLS data encryption.• <i>NONE</i>: Turn off TLS encryption. |

Analyze limits parameters

The *analyze limits* parameters define thresholds used for the *central manager limits* tile on the Deployment Health Dashboard and elsewhere. For more information, see [Deployment health dashboard](#).

| Parameter | Value Type | Description |
|---|------------|-----------------------|
| CLASSIFIER_MEMORY_USAGE_THRESHOLD | Integer | Valid values: 1 - 100 |
| HTTP_GIMSERVER_AUTH_CONNECTIONS_THRESHOLD | Integer | Valid values: 1 - 100 |
| HTTP_GIMSERVER_CONNECTIONS_THRESHOLD | Integer | Valid values: 1 - 100 |
| HTTP_GUI_CONNECTIONS_THRESHOLD | Integer | Valid values: 1 - 100 |
| MYSQL_CONNECTIONS_THRESHOLD | Integer | Valid values: 1 - 100 |
| OPEN_HANDLERS_THRESHOLD | Integer | Valid values: 1 - 100 |
| RUNNING_PROCESSES_THRESHOLD | Integer | Valid values: 1 - 100 |
| UNAUTHENTICATED_CONNECTIONS_THRESHOLD | Integer | Valid values: 1 - 100 |

CyberArk parameters

| Parameter | Value Type | Description |
|-------------------------------|------------------|---|
| CYBERARK_USER_NAME | String | Updates the CyberArk user name. |
| CYBERARK_USER_PASSWORD | Encrypted String | Updates the encrypted CyberArk vault user password. |
| CYBERARK_VAULT_WEBSERVER_NAME | String | Updates the CyberArk vault web server name. |

Classification parameters

| Parameter | Value Type | Description |
|----------------------------|------------|--|
| classifier_running_timeout | Integer | Sets a time limit, in minutes, for the housekeeping process (nanny). After the timeout period, the nanny considers the classifier process to be inactive and restarts it.
Valid values: 5 - 720
Default = 30 |
| classifier_gather_data | Boolean | Enables or disables the gathering of system data.
Valid values: <ul style="list-style-type: none">• 0: gathering of system data is disabled• 1: gathering of system data is enabled |
| compare_max_row_threshold | Integer | Changes the display threshold value.
Default and maximum value: 1000 rows |

Classifier examples

Use the following example to modify the value of the classifier_running_timeout parameter.

```
>grdapic modify_guard_param paramName=classifier_running_timeout paramValue=50
```

Use the following example to modify the value of the classifier_gather_data parameter.

```
>grdapic get_guard_param paramName=classifier_gather_data
ID=0
classifier_gather_data value: false

>grdapic modify_guard_param paramName=classifier_gather_data paramValue=1
ID=0
ok

>grdapic get_guard_param paramName=classifier_gather_data
ID=0
classifier_gather_data value: true
ok
```

Use the following example to view and modify the value of the compare_max_row_threshold parameter.

```
grdapi get_guard_param paramName=COMPARE_MAX_ROW_THRESHOLD
ID=0
COMPARE_MAX_ROW_THRESHOLD value: 1000
ok

grdapi modify_guard_param paramName=COMPARE_MAX_ROW_THRESHOLD paramValue=91935
modify_guard_param:
ERR=5059
Error Parameter Value is greater then MAX allowed : 1000
Error in modify_guard_param. Can not process the request
ok

grdapi modify_guard_param paramName=COMPARE_MAX_ROW_THRESHOLD paramValue=999
ID=0
ok

grdapi get_guard_param paramName=COMPARE_MAX_ROW_THRESHOLD
ID=0
COMPARE_MAX_ROW_THRESHOLD value: 999
ok
```

Data mart parameters

| Parameter | Value Type | Description |
|---|------------|---|
| COPYFILE_THREAD_POOL_CORE_SIZE | Integer | For internal use only, tunes the size of the data mart threadpool. |
| COPYFILE_THREAD_POOL_IDLE_KEEP_ALIVE_TIME_SEC | Integer | For internal use only, tunes the size of the data mart threadpool. |
| COPYFILE_THREAD_POOL_MAX_SIZE | Integer | For internal use only, tunes the size of the data mart threadpool. |
| COPYFILE_THREAD_POOL_MAX_TASKS_WAITING | Integer | For internal use only, tunes the size of the data mart threadpool. |
| CUSTOM_DATAMART_FILE_REMOVE_EXTRA_BACKSLASH | Binary | Removes an extra backslash from custom data mart files during extraction. |

Datasource parameters

| Parameter | Value Type | Description |
|---|------------|--|
| allow_datasource_full_control_by_role | Boolean | Controls whether assigning a role on a datasource gives the role full control over the datasource.
Valid values: <ul style="list-style-type: none">• false• true Default = false |
| customtable_running_timeout | Integer | Sets a timeout mechanism, in minutes, for a hung custom table data upload. When a datasource hangs, the custom data upload stops after the timeout period and skips to the next datasource in the queue. |
| DATASOURCE_CONFIRMATION_EXPIRATION_TIME | Integer | To delete a datasource (or a set of datasources) a confirmation number is required. By default the confirmation number expires after 5 minutes. Use this parameter to change the expiration time to between 4 to 60 minutes. |
| MIN_OPTIMIZE_SIZE | Integer | For a specified database, sets the minimum size for optimization. The size must be between 1000 and 10000000. |

Datasources example

Use the following command to modify the value of the customtable_running_timeout parameter.

```
grdapi modify_guard_param paramName=allow_datasource_full_control_by_role paramValue=true customtable_running_timeout
paramValue=5
```

Use the following command to modify the value of the datasources parameters.

```
grdapi modify_guard_param paramName=customtable_running_timeout paramValue=5
```

Health analyzer parameters

These parameters control the predictions of DB sizes and files on disk (/var). For more information, see [DB sizes and files on disk \(/var\)](#).

| Parameter | Value Type | Description |
|-------------------------------------|------------|--|
| HEALTH_ANALYZER_DB_LOOKAHEAD_DAYS | Integer | Alerts are sent if the HEALTH_ANALYZER_DB_USAGE_THRESHOLD is predicted to occur in the next HEALTH_ANALYZER_DB_LOOKAHEAD_DAYS.
Default = 14 |
| HEALTH_ANALYZER_DB_SAMPLE_DAYS | Integer | The number of immediately preceding days that the DB growth is monitored. Use this parameter to predict future usage.
Default = 7 |
| HEALTH_ANALYZER_DB_USAGE_THRESHOLD | Integer | The DB size threshold (in %) at which an alert is sent. 100% size varies according to the Guardium system type (50% of /var for collector, and 75% of /var for aggregator).
Range is 1 - 100%. Default = 50 |
| HEALTH_ANALYZER_VAR_LOOKAHEAD_DAYS | Integer | Alerts are sent if HEALTH_ANALYZER_VAR_USAGE_THRESHOLD is predicted to occur in the next HEALTH_ANALYZER_VAR_LOOKAHEAD_DAYS.
Default = 14 |
| HEALTH_ANALYZER_VAR_SAMPLE_DAYS | Integer | Number of days the /var growth is monitored. Use this parameter to predict future usage.
Default = 7 |
| HEALTH_ANALYZER_VAR_USAGE_THRESHOLD | Integer | The /var size threshold (in %) at which an alert is sent.
Range is 1 - 100%. Default = 50 |

Inspection engine parameters

Before you configure the Database Discovered Instances Rules in the GUI, you need to enable inspection engine creation by setting the IE_CREATION parameter to 1. For more information, see [Database discovered instances rules](#) and [apply_rules_on_discoveredinstances](#).

| Parameter | Value Type | Description |
|------------------------|------------|---|
| IE_CREATION | Boolean | Required for automatic inspection engine creation. Determines whether Guardium automatically creates inspection engines on a collector, based on whether inspection engine creation is enabled on the Database Discovered Instances Rules page.
Valid values: <ul style="list-style-type: none">• 0 (false): Disable automatic inspection engine creation.• 1 (true): Enable automatic inspection engine creation, according on the rules selected on the Database Discovered Instances Rules page. Default = 0 (false) |
| IE_PROCESSED_TIMESTAMP | Date | Timestamp for identifying already considered, discovered instances for IE creation functionality. |

Offline help parameters

To use IBM Documentation without requiring an internet connection, you can use IBM® Documentation Offline to access help files for Guardium and other IBM products. IBM Documentation Offline allows you to view IBM Documentation either as a desktop application or from your corporate intranet. For more information about installing and using IBM Documentation Offline, see <https://www.ibm.com/docs/en/offline>.

After installing and configuring IBM Documentation Offline, use the following parameters to enable IBM Documentation Offline with Guardium.

| Parameter | Value Type | Description |
|--------------|------------|--|
| HELP_DISABLE | Boolean | Enable or disable IBM Documentation Offline for Guardium help links. The setting is disabled by default.
Valid values: <ul style="list-style-type: none">• 0 (false): Disable IBM Documentation Offline. When disabled, the Guardium system uses help files from the public IBM Documentation site. This is the default behavior.• 1 (true): Enable IBM Documentation Offline. When enabled, the Guardium system links to help files from the IBM Documentation Offline instance identified by the HELP_HOST and HELP_PORT parameters. |
| HELP_HOST | String | Specify the host name of the system where IBM Documentation Offline is installed. If you leave the server name blank, the online help is directed to www.ibm.com . |
| HELP_PORT | String | Specify the port number for the IBM Documentation Offline configuration. The default value is 443. |

Offline help parameters examples

- The following example uses the GuardAPI to find and set the host name,

```
grdapic get_guard_param paramName=HELP_HOST  
ID=0  
HELP_HOST value: test.mycompany.com  
  
grdapic modify_guard_param parameter_name=HELP_HOST parameter_value=test.mycompany.com
```

- The following example uses the GuardAPI to set the port value,

```
grdapic modify_guard_param paramName=HELP_PORT paramValue=9443
```

Manage SQL parameters

These parameters allow you to manage various SQL details.

| Parameter | Value Type | Description |
|--------------------------|------------|--|
| ALERT_OBJECT_NUM_LIMIT | Integer | Maximum number of SQL objects in one alert message for an object template variable. |
| DB2_COMMAS_DECIMAL_POINT | Integer | Flag for the ANTLR3 DB2 parser to consider a comma as a numeric precision mark. |
| DUMP_DATA_FOR_FORENSICS | Integer | Determines whether to dump full SQL details into the Kafka server. The full SQL details are used for forensics and analysis. Valid values: <ul style="list-style-type: none">• 0 (off): Do not dump full SQL details• 1 (on): Dump full SQL details Default = 0 |
| LONG_VALUE_SPLIT_IN_CCSV | Binary | Allows text to be split into multiple lines during CSV export. |
| MAX_SAVED_CONSTRUCTS | Integer | Size of the SQL construct rule. Results are being saved in the session. |

Nanny parameters

These parameters enable and configure sending test messages to the alerter orrsyslog to verify that it is communicating with Guardium.

| Parameter | Value Type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value Type | Description |
|------------------------------|------------|---|
| GENERATE_TOMCAT_DUMP | Binary | Triggers Tomcat core dump. |
| NANNY_ALERT_RSYSLOG | Integer | Controls whether the nanny monitors rsyslog servers. |
| NANNY_ALERT_RSYSLOG_FREQ | Integer | Determines the frequency, in hours, with which the nanny monitors rsyslog servers. |
| NANNY_SNIF_CORE | Integer | Captures the nanny snif core count. Default = 0 (disabled)
A value of 1, 2, or 3 indicates the number of compressed and encrypted cores to save to the /var/IBM/Guardium/log/snif/cores directory as tar files.

Use the fileserver CLI command to upload the compressed snif core tar file. |
| NANNY_TEST_RSYSLOG | Integer | Determines whether the nanny process sends test messages to rsyslog. Valid values: <ul style="list-style-type: none">• 0 (false): Do not send test messages to rsyslog• 1 (true): Send test messages to rsyslog
Success messages are severity <i>info</i> , and error messages are severity <i>med</i> (<i>error</i>).

Default = 1 |
| NANNY_TEST_RSYSLOG_FREQ | Integer | Determines the frequency, in hours, with which the nanny sends test messages to rsyslog.
Default = 0, which sets the frequency to 5 minutes. |
| NANNY_TEST_SMTP_ALERTER | Integer | Determines whether the nanny process checks the status of the SMTP alerter.
If set to 1 (true), the nanny establishes that connectivity is available to the SMTP relay server on the server side and reports the results to Syslog. Success messages are severity <i>info</i> , and error messages are severity <i>med</i> (<i>error</i>).

If the SMTP alerter is down, Guardium attempts to restart it, and reports to Syslog indicating success or failure.

Valid values: <ul style="list-style-type: none">• 0 (false): Do not test the alerter• 1 (true): Test the alerter
Default = 1 |
| NANNY_TEST_SMTP_ALERTER_FREQ | Integer | Determines the frequency, in hours, with which the nanny tests the alerter.
Default = 0, which sets the frequency to 5 minutes. |

Quartz scheduler parameters

These parameters provide input to the Quartz Job Scheduler.

| Parameter | Value Type | Description |
|-----------------------------------|------------|--|
| QUARTZ_LONG_RUNNING_JOB_THRESHOLD | Integer | Defines the Quartz Scheduler long running job threshold in minutes.
Default = 600 (minutes). |
| QUARTZ_MAX_LONG_RUNNING_JOBS | Integer | Defines the maximum number of long running Quartz Scheduler jobs that is considered unhealthy.
Default = 3. |
| QUARTZ_SCHD_ENABLE_MONITOR | Boolean | Enable Quartz Scheduler monitoring.
The default is 0 (off).

To turn on, set to 1. |

Smart card parameters

This configuration is for logging into the Guardium UI using a smart card. For more details, see [Enabling smart card authentication](#).

| Parameter | Value Type | Description |
|--------------------------|------------|---|
| ENABLE_OCSP_CHECK | Binary | Check certificate status via OCSP if smart card authentication is turned on. |
| SMART_CARD_MAPPING_REGEX | String | Sets the value of the regular expression (regex) in the Guardium Portal page to match the user information on a smart card. |

Smart card example

Use the following command to modify the value of the SMART_CARD_MAPPING_REGEX parameter.

```
grdapic modify_guard_param paramName=SMART_CARD_MAPPING_REGEX paramValue="CN=?(.*) ,?OU=?Test Agency ,?OU=?Test Department ,?O=?Test Government ,?C=?US"
```

Sniffer parameters

Use the following parameters to manage Sniffer settings.

| Parameter | Value Type | Description |
|----------------------|------------|---|
| ACTIVE_PARSER_ENGINE | Integer | Controls which parser engine snif will use. Options are: <ul style="list-style-type: none">• 1 - Use ANTLR3 with errors re-parsed by ANTLR2 (default)• 2 - Use ANTLR2• 3 - Use ANTLR3 |

| Parameter | Value Type | Description |
|--------------------------------------|------------|---|
| HOST_SERVICE_OS_NAME_CACHE_SIZE | Integer | Allows you to change the size of sniffer held values in host name, service name, or OS user name caches. Default = 2048.

The cache size must be between 1 and 25000. |
| INTERNAL_REST_CLIENT_SECRET | Encrypted | The internal REST client secret to allow snif and other components to make internal REST calls. |
| INTERNAL_REST_CLIENT_SECRET_PASSWORD | Encrypted | The password for the internal REST client user. |
| LOG_GENERAL_RESPONSE_LENGTH | Number | Displays whether the store_log_general_response_length CLI command is enabled or disabled. Default = disabled |
| PE_TRAINING_PHASE_ONE_LENGTH | Integer | Minimum mandatory training period (in days) for the snif probability engine. |
| PE_TRAINING_PHASE_TWO_LENGTH | Integer | Minimum training period (in hours) where snif must see no new training data. Extended dynamically when new events are encountered. |
| SAVED_RESPONSE_QUEUE_SIZE | Integer | Allows you to change the queue size for saved responses. |
| SELECTIVE_AUDIT_PRESCREEN_THRESHOLD | Integer | Snif internally disables the prescreen functionality for performance purposes if total selective audit group member count exceeds this value. |
| SNIF_DQ_ARE_LITERALS | Integer | Controls which database types snif will consider double quoted strings literals by default. |
| SNIF_USE_FEED_ANALYZER_THREAD | Integer | Snif use feed analyzer thread. |
| UID_CHAIN_PROCESS_ASYNC | Integer | Control synchronous/asynchronous processing of the UID CHAIN in snif. |

SNMP parameters

Use the following parameters to set certain system SNMP settings.

| Parameter | Value Type | Description |
|-------------------------------|------------|--|
| GUARDIUM_SNMP_TR_AP_MSG_OID | String | The message for the Guardium SNMP trap OID. The default message is .1.3.6.1.4.1.18708.1.6 . |
| GUARDIUM_SNMP_TR_AP_OID | String | Specify the Guardium SNMP trap OID. Use this parameter to change how the Alerter sends SNMP traps to older values or to another value that you need to work with a particular server that monitors SNMP traps. For more information, see Configuring the alerter .

The default trap OID is .1.3.6.1.4.1.18708.1.1.1 |
| SNMP_AUTHENTICATION_PASSWORD | Encrypted | SNMP authentication passphrase. |
| SNMP_ENCRYPTION_PASSWORD | Encrypted | SNMP encryption passphrase. |
| SNMP_ENGINE_ID | String | If required, change the SNMP engine ID. Use the show system snmp engineid CLI command to see the current engine ID. Note: Engine ID must be unique. |
| SNMP_USER_AUTHENTICATION_TYPE | String | SNMP user authentication type for v3. |
| SNMP_USER_ENCRYPTION_TYPE | String | SNMP user encryption type for v3. |
| SNMPV3_USER | String | Create a new SNMP version 3 user account. Guardium recommends that you use the store_system_snmp_user CLI command to create a new user. |
| SNMP_VERSION | String | Set the SNMP version for this machine. Valid values = v2c or v3 |

Syslog TCP parameters

These parameters manage TPC reception in syslog.

| Parameter | Value Type | Description |
|---------------------------|------------|--|
| SYSLOG_TCP_RECEPTION_ON | Integer | Controls whether syslog TCP reception is on. Default = 1 (off)

Set to 0 to turn on. |
| SYSLOG_TCP_RECEPTION_PORT | Integer | Specify the port to use for syslog TCP reception. Default = 10514.

The port number must be between 1 and 65535. |

Threat analytics parameters

| Parameter | Value Type | Description |
|---------------------------------------|------------|--|
| EI_FAILED_LOGIN_DB_USER_THRESHOLD | Number | The database user threshold for threat analytics failed log ins. Default = 2. |
| EI_FAILED_LOGIN_DISPLAY_DB_USER_LIMIT | Number | The number of different database users threshold for a failed threat analytics login case. Default = 2. |
| EI_FAILED_LOGIN_PER_DB_USER_THRESHOLD | Number | The number of failed log ins per database user threshold for a failed threat analytics login case. Default = 10. |
| EI_GRANT_DORMANT_WEEKS_DEFINITION | Number | The number of weeks without activity to register a user as dormant for threat analytics. Default = 8. |
| EI_SQL_TIMEOUT_IN_SECONDS | Number | Timeout, in seconds, for executing threat analytics scanners on a query or stored procedure. Default = 300. |

Vulnerability Assessment parameters

| Parameter | Value Type | Description |
|-----------------------------------|------------|---|
| ALLOW_NULL_SERVICE_FOR_VA_SUMMARY | Binary | Name for the VA summary.
Set as DEFAULT in case of NULL in service. |
| INAPPLICABLE_TEST_RESULT_STATUS | Binary | Allows you to include or exclude test scores for unsupported database versions from the vulnerability assessment test report.

0: excludes tests with results that have the test score "NOT APPLICABLE".

1: includes tests with results that have the test score "NOT APPLICABLE".
Tip: For vulnerability assessment tests with a defined range of supported database versions, the test returns a score of "NOT APPLICABLE" when the datasource version is not within the range. |
| SAVE_TEST_RESULT_DETAIL_STRING | Binary | Controls detailed information of a test result.

Default = true, include detail information in the test result.

If false, the detail information is not included in the test result. |

Other parameters

| Parameter | Value Type | Description |
|--|------------|---|
| CM_HEALTH_VIEW_HOSTNAME | String | For the cross-CM health view. Hostname of the central manager that the machine is reporting to.

Note:
12.0 You can unregister central managers from the cross-CM health view system by providing an empty <code>paramValue</code> for <code>CM_HEALTH_VIEW_HOSTNAME</code> . Unregistered systems still appear on the aggregated health views of the cross-CM health view system, but their data is no longer updated and their status may not be listed accurately.

<code>grdapi modify_guard_param paramName=CM_HEALTH_VIEW_HOSTNAME paramValue=</code>

12.1 and later You can unregister 12.1 central manager from the cross-CM health view system by providing the central manager name.

<code>grdapi unregister_unit unitIplist=""</code>

To register a central management unit with version earlier to 12.1 and cross-CM health view with version 12.1, use the following API:

<code>grdapi modify_guard_param paramName=CM_HEALTH_VIEW_HOSTNAME paramValue=<CM of CMs hostname></code>

From 12.1, Guardium populates <code>CM_HEALTH_VIEW_HOSTNAME</code> during registration and it cannot be modified. |
| ENABLE_GUARDIUM_INSIGHT_STREAMING | Binary | For Guardium Insight streaming. Enable or disable data streaming to Guardium Insights.

Valid values: <ul style="list-style-type: none">• True: Enable Insights streaming• False (default): Disable Insights streaming |
| ESCAPE_FOR_ARCSIGHT | Binary | Deprecated. |
| FUTURE_PARTITION_EXPAND_DELAY_HOURS | Integer | The maximum number of hours to delay before creating future partitions. Change this parameter only on advice of Guardium Technical Support.
Default = 0. |
| INFORMIX_SAVED_RESPONSE_QUEUE_SIZE | Integer | Informix queue size for the Save response. |
| KEEP_NUMBER_OF_JAVACORE_BUNDLE | Integer | The number of javacore file bundles to keep. The number must be between 1 and 30. Default = 3. |
| LDAP_CONN_TIMEOUT_MILLISEC | Integer | Sets the number of milliseconds before the LDAP test connection times out.
Default = 5000 (5 seconds)

The value must be between 1000 and 300000 ms. |
| LOG_TO_APP_USER | String | Log specified attributes to the Application User field. |
| PASSWORD_MIN_DAYS | Integer | The minimum days required between a password change. Default = 1 (day). |
| PATCH_PRESERVATION | Integer | Controls whether to preserve failed patches. When set to 1 (on), if the patch fails, you can make corrections and then rerun the patch without having to download it again.
Default = 0 (off). |
| REMOTE_FILETRANSFER_RESERVED_SPACE_GB | Integer | The minimum reserve disk space required in remote file transfer between Guardium Data Protection and Guardium Insights. Default = 25. |
| SIZE_OF_RAW_STATEMENT_MAP | Integer | Controls the size of the raw statement map. To view the current size of the raw statement map, use the <code>get_guard_param</code> command. For example:

<code>>grdapi get_guard_param paramName="SIZE_OF_RAW_STATEMENT_MAP"</code>

Default = 2048 |
| 12.1 and later UNIVERSAL_CONNECTOR_CONFIGURATION_FLOW_FLEXTURE | Integer | When set to 1, allows you to use the <code>load_all_packages</code> API to load the universal connector package configuration from a specified folder. |
| WAF_F5_METHOD | Integer | Customer-specific parameter. No longer used. |

| Parameter | Value Type | Description |
|-------------------|------------|---|
| WKC_CONFIGURATION | Encrypted | For internal use only. When decrypted, displays the configuration parameters for the IBM Cloud Pak® for DataIBM Knowledge Catalog integration with Guardium. For more information, see Integrating with IBM Knowledge Catalog for federated data protection . |

Related concepts

- [Database discovered instance rules](#)
- [Datasource APIs](#)
- [System CLI Commands](#)

Related tasks

- [Enabling smart card authentication](#)

Related reference

- [get_all_modifiable_guard_params](#)
- [get_guard_param](#)
- [Classification APIs](#)
- [Health analyzer APIs](#)

Related information

- [DB sizes and files on disk \(/var\)](#)

modify_oauth_validity

This API is available in Guardium V11.2 and later.

GuardAPI syntax

```
modify_oauth_validity parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------------|------------|-------------|
| client_id | String | Required. |
| validity_in_seconds | Integer | Required. |

modify_schedule

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/schedule
```

GuardAPI syntax

```
modify_schedule parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|-------------|
| cronString | String | Required. |
| jobGroup | String | Required. |
| jobName | String | Required. |
| startTime | Date | |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

modify_va_summary_key

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/modify_va_summary_key
```

GuardAPI syntax

```
modify_va_summary_key parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------------|------------|--|
| allowNullsServerName | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| useDatasourceName | Boolean | Required. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| useHost | Boolean | Required. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| usePort | Boolean | Required. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| useServiceName | Boolean | Required. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |

must_gather

This command collects information on the state of the Guardium system for use by Guardium Support.

For more information, see [Basic information for IBM Support](#).

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/must_gather
```

GuardAPI syntax

```
must_gather parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| commandsList | String | Required. The information to gather. For valid values, call must_gather from the command line with --help=true. For more information, see Running must_gather from the CLI . |
| description | String | A description of the issue. |
| email | String | Email address for results.
If you specify an email, the logs are gathered for 10 minutes from the time you start the process and an email is sent afterward. |
| maxLogLength | Integer | Maximum number of rows to appear in the log. |
| pmrNumber | String | The PMR number for this issue. |
| runDuration | Integer | The length of time, in minutes, to gather information.
Default = 10 (minutes) |
| startRun | Date | Time to start the run. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GuardAPI example

```
grdapi must_gather commandsList="alert_issues" description="Issues with real-time alerts"
```

Related concepts

- [Basic information for IBM Support](#)

non_credential_scan

Use this command to submit jobs that scan databases within the serversGroup for enabled default users in the usersGroup.

Submitted jobs run under the Classifier Listener and can be tracked in the Job Queue report. For more information, see the [Default DB Users Enabled](#) report in [Predefined admin reports](#).

Note: To cancel a submitted job from the Job Queue report, right-click the job name and select **Stop Job**.

Note: If a server within the serversGroup cannot be reached, an exception of type Scheduled Job Exception is added and the server is not scanned.
This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
non_credential_scan parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------|------------|--|
| databaseType | String | Required. The database type. Valid values are: <ul style="list-style-type: none">• DB2• IBM ISERIES• INFORMIX• MS SQL SERVER• MYSQL• NETEZZ• ORACLE• POSTGRESQL• SYBASE• TERADATA |
| serversGroup | String | Required. A valid group of servers (Server IP/Instance Name/Port) as defined with Group Builder. |
| usersGroup | String | Required. A valid group of users (DB User/DB Password) as defined with Group Builder. Default groups exist within Group Builder. |

Example

```
grdapi non_credential_scan databaseType=ORACLE serversGroup=oracleServers usersGroup="ORACLE Default Users"
```

Related concepts

- [Predefined admin reports](#)

nscd

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
nscd parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| state | String | |

patch_cleanup

This command deletes all the patches with the suffixes "enc" or "sig" in the patches directory .

This API is available in Guardium v11.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/patch_cleanup
```

GuardAPI syntax

```
patch_cleanup parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

patch_install

Use this API to install a Guardium patch. The patch number is required.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/patch_install
```

GuardAPI syntax

```
patch_install parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| mode | String | Valid values: <ul style="list-style-type: none">• <i>local_only</i>• <i>pull_only</i>• <i>pull_install</i> |
| patch_date | Date | A date and time in the format <i>yyyy-mm-dd hh:mm:ss</i> or a relative time such as <i>NOW +2 HOUR</i> . <ul style="list-style-type: none">• If <i>patch_date</i> is left blank or contains a date in the past, then Guardium installs the patch within 5 minutes after the command is called.• If <i>patch_date</i> is a future date and time, then the patch is installed within 5 minutes of the assigned date and time. For more information about date formats, see Dates and Timestamps . |
| patch_number | Integer | Required. |
| unitIpList | String | Required. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• <i>all_managed</i>: execute on all managed units but not the central manager• <i>all</i>: execute on all managed units and the central manager• <i>group:<group name></i>: execute on all managed units identified by <i><group name></i>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

The following examples install patch number 4000 onto the test.guard.ibm.com machine in four hours. The first example uses the GuardAPI, the second example shows the REST API.

```
grdapi patch_install patch_number=4000, api_target_host=test.guard.ibm.com patch_date="NOW +4 HOUR"
curl -k --header "Authorization: Bearer ed272932-28e6-4b56-80a3-664e5e0220de" -i -H "Content-type: application/json" -X PUT -d
{"patch_number": "4000", "api_target_host": "test.guard.ibm.com", "patch_date": "NOW +4 HOUR"}
```

pause_or_resume_job

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/schedule
```

GuardAPI syntax

```
pause_or_resume_job parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| jobGroup | String | Required. |
| jobName | String | Required. |
| pause | Boolean | Required. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

pause_or_resume_scenarios

This command allows you to manage and schedule Discover Sensitive Data scenarios in batch. You can specify a set of scenarios by using a pattern, and then pause, restart, and preview the output.

This API is available in Guardium v11.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/schedule
```

GuardAPI syntax

```
pause_or_resume_scenarios parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------------|------------|---|
| pause | Boolean | <p>Required. Acts the same way as Activate schedule in the Discover Sensitive Data Scenario definition. Valid values:</p> <ul style="list-style-type: none"> • 0 (false, pause a running job) • 1 (true, resume a paused schedule) <p>Default = 1 (true)</p> |
| preview | Boolean | <p>Run the command without applying any changes to see which scenarios are selected for a given scenarioNamePattern and make changes as needed. Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true) <p>Default = 0 (false)</p> |
| scenarioNamePattern | String | <p>Required. Specify Discover Sensitive Data scenario names using MySQL patterns. For example, underscores (_) and percent signs (%) are accepted, but an asterisk (*) is not.</p> <p>All scenarios that meet the specified criteria run when pause = 1.</p> |
| verbose | Boolean | <p>Controls the amount of information displayed in the output. Valid values:</p> <ul style="list-style-type: none"> • 0 (false, less verbose) • 1 (true, more verbose) <p>Default = 0 (false)</p> |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related tasks

- [Discover Sensitive Data](#)

policy_fam_rule_delete

This command deletes the specified rule from the specified FAM policy.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/famPolicyRule
```

GuardAPI syntax

```
policy_fam_rule_delete parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|---|
| policyName | String | Required. |
| ruleName | String | Required. Name of the rule to be deleted. |

Examples

To delete a rule named audit_read in the policy named fam26:

```
policy_fam_rule_delete policyName=fam26 ruleName=audit_read
```

Related concepts

- [FAM discovery and classification in Windows and UNIX-Linux file servers](#)
- [Using rules for file activity policies](#)

Related reference

- [delete_policy](#)
- [enable_fam_crawler](#)
- [disable_fam_crawler](#)
- [add_action_to_fam_rule](#)
- [create_fam_rule](#)
- [get_fam_crawler_info](#)
- [create_policy](#)
- [list_policy_fam_rule](#)

policy_install

This command installs one or more policies.

Specify multiple policies by using a pipe (|) character as a delimiter between policy names. Specify the policies in the order that you want to install them.

Note: If you change one or more policies, you must reinstall all policies.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/policy_install
```

GuardAPI syntax

```
policy_install parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| policy | String | Required. The name of the policy or policies to install. Use a pipe () character to separate multiple policies. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

The following example installs three policies.

```
grdapi policy_install policy="policy 20|policy 30|policy 40"
```

Related tasks

- [Creating and installing a policy and policy rules](#)

Related reference

- [policy_uninstall](#)

policy_uninstall

This command uninstalls a policy.

This API uninstalls a policy, but does not delete it.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/policy_uninstall
```

GuardAPI syntax

```
policy_uninstall parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| policy | String | Required. The name of the policy to uninstall. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi policy_uninstall policy="policy 20"
```

Related reference

- [delete_policy](#)

- [policy_install](#)

populateMembersForGroup

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/populateMembersForGroup
```

GuardAPI syntax

```
populateMembersForGroup parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| dcName | String | Required. |
| groupName | String | Required. |

populate_from_dependencies

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
populate_from_dependencies parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------------|------------|--|
| descOfEndingGroup | String | Required. |
| descOfStartingGroup | String | Required. |
| flattenNamespace | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| getFunctions | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| getJavaClasses | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| getPackages | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| getProcedures | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| getSynonyms | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |

| Parameter | Value type | Description |
|------------------------|------------|---|
| getTables | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| getTriggers | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| getViews | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| isAppend | Boolean | Required. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| isEndingGroupQualified | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| reverseIt | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| selectedDataSourceName | String | Required. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

populate_group_from_query

This command populates a group from an existing query.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/group_query
```

GuardAPI syntax

```
populate_group_from_query parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|---|
| activateSchedule | Boolean | Activates the schedule specified by cronString. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |

| Parameter | Value type | Description |
|-----------------|------------|---|
| clearGroup | Boolean | Required. Valid values: <ul style="list-style-type: none"> 0 (false). Append new members to the group. 1 (true). Clear the existing members from the group before adding new members. |
| cronString | String | The schedule to run the query as a cron string. For example, to run the query every day at 2 AM:
<pre>0 2 * * *</pre> . |
| groupDesc | String | Required. A description of this group. |
| queryColumns | String | Required. The names of the columns to import into the group as a comma-separated string. For tuples, specify one column per tuple. |
| queryName | String | Required. The name of the query to use for populating the group. The query must already exist. |
| queryParams | String | Parameters for the query (specified as a key = value pair). For example,
<code>QUERY_FROM_DATE=NOW -3 DAY,QUERY_TO_DATE=NOW</code> |
| startDate | Date | The date to start using this API, based on the value of cronString. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> all_managed: execute on all managed units but not the central manager all: execute on all managed units and the central manager group:<group name>: execute on all managed units identified by <group name> host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

proxy

12.1 and later Use this API to create proxy connections. Guardium® supports a web proxy to connect to a remote source that requires a proxy server to connect.

REST API syntax

This API is available as a REST service with the `proxyConfig` method. Call this API as follows:

```
https://[Guardium hostname or IP address]:8443/restAPI/proxy
```

GuardAPI syntax

```
proxy parameter=value
```

Proxy API usage

```
grdapic proxy <options>
  Options: list=true

  clearall=true
    reload=true
  stop=true
    setup=true
  proxy_host=<proxy_server> proxy_port=<proxy_port> target_host=<target_server>
  target_port=<target_port>
    clear=true target_host=<target_server>
  target_port=<target_port> diagnostics=true
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| clear | Boolean | Deletes the proxy connections from the system.
Valid values: <ul style="list-style-type: none"> false true |
| clearall | Boolean | Deletes all the proxy connections from the system.
Valid values: <ul style="list-style-type: none"> false true |

| Parameter | Value type | Description |
|-----------------|------------|--|
| diagnostics | Boolean | Runs diagnostics on all the proxy connections and writes the output to a log file.
Valid values: <ul style="list-style-type: none">• <i>false</i>• <i>true</i>) |
| list | Boolean | Lists the proxy connections.
Valid values: <ul style="list-style-type: none">• <i>false</i>• <i>true</i> |
| proxy_host | String | IP or hostname of the proxy server. |
| proxy_port | String | Port number for the proxy connection. |
| reload | Boolean | Restart and refresh all the proxy connections.
Valid values: <ul style="list-style-type: none">• <i>false</i>• <i>true</i> |
| setup | Boolean | Setup the proxy connection.
Valid values: <ul style="list-style-type: none">• <i>false</i>• <i>true</i> |
| stop | Boolean | Stops all the proxy connections without deleting them from the system.
Valid values: <ul style="list-style-type: none">• <i>false</i>• <i>true</i> |
| target_host | String | Hostname/IP of the target resource for the proxy connection |
| target_port | String | Port number of the target resource for the proxy connection. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• <i>all_managed</i>: execute on all managed units but not the central manager• <i>all</i>: execute on all managed units and the central manager• <i>group:<group name></i>: execute on all managed units identified by <i><group name></i>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>.
IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

Setting up proxy

To configure a proxy for `myhost.example.com:443` via proxy server `proxy.example.com:3128`, use the following command:

```
grdapic proxy setup=true proxy_host=myhost.example.com:443 proxy_port=3128 target_host=proxy.example.com target_port=443
```

Listing target and proxy hosts

To list all the proxy connections, use the following command:

```
grdapic proxy list=true
```

Output: `myhost.example.com:443 via proxy proxy.example.com:3128`

Testing proxy server

To troubleshoot the proxy server, use the following command:

```
grdapic proxy diagnostics=true
```

Output: Please view `log/guard_proxy.txt` using the fileserver.

Verify proxy connection

To verify the proxy connection, use the following command:

```
support show port open <target_server> <target_port>
```

For more information, see [support show port open](#) CLI Command.

pull_external_stap_keystore

This command moves the External S-TAP® keystore between a central manager and its managed units.

This API is available in Guardium V10.6 and later.

The External S-TAP pull_external_stap_keystore command provides a mechanism to populate the External S-TAP keystore from either a central manager or a managed unit.

- To pull the External S-TAP keystore from the central manager to a managed unit, run this API on the managed unit.
- To pull the External S-TAP keystore from the central manager to one or all of the associated managed units, run this API on the central manager.

GuardAPI syntax

```
pull_external_stap_keystore parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI examples

- To pull the keystore from a managed unit to the central manager, run the following command from the managed unit:
`grdapi pull_external_stap_keystore`
- To pull the keystore from the central manager to all associated managed units, run the following command from the central manager:
`grdapi pull_external_stap_keystore`
- To pull the keystore from the central manager to a specific managed unit, run the following command from the central manager:
`grdapi pull_external_stap_keystore api_target_host=hostname`

Related concepts

- [External S-TAP](#)

push_insights_trust

This command pushes a trust certificate from Guardium® Insights to Guardium Data Protection S-TAPs.

The certificate must be in PEM format and include the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- tags.

The certificate chain that you paste needs to be downloaded (from the browser) from the Guardium Insights cluster that is targeted for S-TAP® migration. The certificate is not stored on the managed unit; but on the S-TAP host (database server).

Notes:

- If you run this command from a central manager, you must specify the api_target_host parameter to target a managed unit (because central managers don't have S-TAPs). You can also run this command directly from a collector or stand-alone machine.
- When you call this command as a GuardAPI, leave pemData blank, and follow the directions in the CLI to paste the entire certificate.
- You can push certificates only for UNIX S-TAPs.
- You can also add the Guardium Insights certificate from the Guardium Data Protection GUI. For more information, see the [Send command](#) under [Linux®-UNIX: Configuring S-TAP in the S-TAP Control page](#).

This API is available in Guardium v11.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/push_insights_trust
```

GuardAPI syntax

```
push_insights_trust parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| pemData | String | Required for REST API only. The certificate to send to the S-TAP hosts, in PEM format. <ul style="list-style-type: none">• For a REST API, paste the trusted Guardium Insights certificate in, including the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- tags.• For a GuardAPI, ignore this parameter. The CLI walks you through the required steps. |
| stapHost | String | Required. Specify the name of one or more S-TAP hosts, or specify <i>all_unix_active</i> to send the certificate to all active UNIX S-TAP hosts. For valid values, call <code>push_insights_trust</code> from the command line with <code>--help=true</code> . |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• <i>all_managed</i>: Run on all managed units but not the central manager• <i>group:<group name></i>: Run on all managed units identified by <i><group name></i>• host name or IP address of a managed unit: Specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. <p>Note: IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

The following GuardAPI example runs on a stand-alone machine with a certificate chain that includes two certificates. The pemData parameter is not specified in the command. Follow the directions in the CLI to paste the certificate data in.

```
vm01.mycompany.com> grdapi push_insights_trust stapHost=9.55.254.111
```

The response from the CLI is as follows (be sure to paste in the entire certificate):

```
Please paste your Certificate below in PEM encoded format including tags.  
PEM encoded format should include the '-----BEGIN CERTIFICATE-----' and '-----END CERTIFICATE-----' tags. The Certificate Authority (CA) Root and Intermediate certificate(s) (if applicable) will also need to be pasted at this time for validation purposes. Please ensure that all certificates are in PEM format and include the aforementioned tags. When pasting multiple certificates, please make sure that each certificate is pasted on a new line in the following order:
```

```
-----BEGIN CERTIFICATE-----  
(End-Entity certificate)  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
(Intermediate certificate(s) - if applicable)  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
(Root certificate)  
-----END CERTIFICATE-----
```

```
Once done pasting your certificate(s), press ENTER followed by CTRL-D to continue.
```

```
-----BEGIN CERTIFICATE-----  
MIIDbzCCAlEqAwIBAgIQX+U115HoAr3cToMpY  
...  
01zSjANBgkqhkf+9tfN60rPSFmUp0CDTrew==  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
MIIDMTCCAhmqAwIBAgIQCO/HN2U7x20Fsn4Df  
...  
rBXQ+JoCyEQhZK0cIhhTKGluI7zK0Q=  
-----END CERTIFICATE-----  
ID=0  
Insights data sent to active synchronized S-TAP hosts:  
9.55.254.111  
ok
```

The following REST API example includes the pemData parameter.

```
curl -k --header "Authorization: Bearer hV59gjW71nwY4dAWpNdLi7890" -i -H "Content-Type: application/json" -d '{stapHost:"dev-db01",pemData:"-----BEGIN CERTIFICATE-----\nMIICyDDAbICGGKT3Xa83UY2dPfGpxb7CoR4n7tRMA0GCSqGS1b3DQEBCwUAMDMx\n...\ntla+CH8jyicLx+J9FQri7K1YSiBXznlug61Hlc0AA1TrZOPvvzIsPiPeV+iSalF7w\nojuBlgMxSOfbYVn6Rxcye+u7dJb07TcUSFqtimmx55vmfc3/VwGXJcAqG6Jh7w==\n-----END CERTIFICATE-----"}' -X PUT https://vm04.mycompany.com:8443/restAPI/push_insights_trust
```

Related reference

- [migrate_stap_config](#)

Related information

- [Linux-UNIX: Configuring S-TAP in the S-TAP Control page](#)

push_parameter_to_mu

Push the value of a modifiable parameter from the central manager to a managed unit or group of managed units.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/push_parameter_to_mu
```

GuardAPI syntax

```
push_parameter_to_mu parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| groupname | String | The name of a managed unit group. |
| paramname | String | The name of the parameter to push. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related reference

- [modify_guard_param](#)

quick_search

This REST API is a wrapper for Solr queries, which are used in the Investigation Dashboard. This command is similar to the search command, but has some improvements.

This API is available in Guardium v11.3 and later.

Note: The quick_search API returns codes that represent the titles of the columns (fields) in the returned tables. For example, quick_search might return the following rows:

```
"15": "Failed Login - Alert and Quarantine if Repeated",
      "16": "5",
```

To map the codes ("15" and "16", in this case) to the actual column names, use the [getFieldsTitles](#) API.

REST API syntax

This API is available only as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/quick_search
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| category | String | Required. The Guardium Solr collections. The categories generally map to the categories that are shown in the Investigation dashboard UI.
To view the valid categories, call this REST API with all of the required parameters but enter a clearly invalid value (for example, category=kookoo). Guardium returns all valid values for category. |
| endTime | String | Search for records that were created before the specified endTime. The time must be specified in the format:YYYYMMDD+HH:MM:SS. |
| fetchSize | Integer | The maximum number of records returned by the API. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| filters | String | Filters consume input and produce a stream of tokens. Filters must be in a specific format, for example:

<pre>"filters": "name=Database&value=9.147.31.113:5.6.27&isGroup=false&name=DB User&value=SYSTEM&isGroup=false&name=Server&value=9.147.31.113&isGroup=false"</pre> For more information about filters, see the Apache Solr Reference Guide > Schema and Indexing Guide . |
| firstPosition | Integer | The position in the result. Can be used together with fetchSize to iterate through the results. |
| inputTZ | String | The initials of a timezone, such as UTC or EST. If provided, startTime and endTime parameters are converted from that timezone to the Guardium appliance's timezone before the search is executed. All date fields in the results are converted from Guardium appliance's timezone to the inputTZ timezone provided before the results are returned.
To view the valid timezone codes, call this REST API with all of the required parameters but enter a clearly invalid value (for example, inputTZ=kookoo). Guardium returns all valid values for inputTZ. |
| pivotBy | String | |
| query | String | A Solr query. You can use this parameter to write free-form Solr query expressions. For more information, see the Apache Solr Reference Query Guide . |
| startTime | String | Search for records that were created after the specified startTime. The time must be specified in the format: YYYYMMDD+HH:MM:SS . |
| summaryBy | String | Group results by the selected field code. You can specify up to 2 field title codes to group by.
Note: To map the field codes to column names, use the getFieldsTitles API. |
| withFacets | String | Include facets in the search. For more information, see Investigation dashboard for data or Investigation dashboard for files . Valid values are: <ul style="list-style-type: none">• 0 (Off: Do not include facets)• 1 (On: Include facets) Default = 0. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

```
curl -k --header "Authorization: Bearer <token>" -i -H "Content-Type: application/json" -X POST --data '
{"category": "ERROR", "inputTZ": "UTC", "startTime": "20201019 00:00:01", "endTime": "20221225 10:11:11",
*"filters": "name=Server&value=9.55.205.70&isGroup=false"*)
' <Guardium host>:8443/restAPI/quick_search" class="external-link" rel="nofollow">https://<Guardium
host>:8443/restAPI/quick_search
...
...
{
  "2": "DB2_ZZ7I", "13": "2022-03-23 10:02:45", "3": "9.55.205.70", "14": "SESSION_GUESS", "_shard_": "my_company.com", "6":
  "9.55.205.70", "7": "DB2", "8": "2022-03-23", "9": "14:02:45", "id": "3" }

curl -k --header "Authorization: Bearer <token>" -i -H "Content-Type: application/json" -X POST --data '
{"category": "ERROR", "inputTZ": "UTC", "startTime": "20201019 00:00:01", "endTime": "20221225 10:11:11",
"filters": "",*,*,"query": "Server=9.55.205.70 AND DB_Type=DB2"*, "fetchSize": "1000"
}

' https://<Guardium host>:8443/restAPI/quick_search
...
...
{
  "2": "DB2_ZZ7I", "13": "2022-03-23 10:02:45", "3": "9.55.205.70", "14": "SESSION_GUESS", "_shard_": "my_company.com", "6":
  "9.55.205.70", "7": "DB2", "8": "2022-03-23", "9": "14:02:45", "id": "3" }
```

Use the [getFieldsTitles](#) REST API to map the column codes to column names. For example:

```
curl -k --header "Authorization: Bearer <token>" -i -H "Content-Type: application/json" https://il-
vm01.isslab.usga.ibm.com:8443/restAPI/fieldsTitles
...
...
"0": "lucene.field.category",
"1": "OS User",
"2": "DB User",
"3": "Client IP",
"4": "Source Program",
"5": "Client Host name",
"11;12": "Object Verb",
"6": "Server",
"7": "DB Type",
"8": "Date",
"9": "Time",
...
```

Related concepts

- [Investigation Dashboard](#)

Related reference

- [getFieldsTitles](#)
- [search](#)

reboot_image_universal_connector

After you run this grdapi, the UC stops the container that is currently running and starts a new one, which is loaded from the UC image that comes with the installation.

This API is available in Guardium v11.4 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/restoreUniversalConnectorImage
```

GuardAPI syntax

```
reboot_image_universal_connector parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related concepts

- [Guardium universal connector](#)

refresh_quick_search_groups

This command sends all defined groups to the specified target hosts. Use it when you have defined a new group(s) on the central manager, but the scheduled time for the central manager to update its managed units has not yet occurred.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
refresh_quick_search_groups parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To update the groups on all managed units:

```
grdapi refresh_quick_search_groups
```

Related concepts

- [Investigation dashboard](#)

Related reference

- [Investigation dashboard APIs](#)

refresh_stap_info

Run this command to refresh the S-TAP configuration from the agent.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/refresh_stap_info
```

GuardAPI syntax

```
refresh_stap_info parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| stapHost | String | Required. IP or hostname of the S-TAP® host. For valid values, call <code>refresh_stap_info</code> from the command line with <code>--help=true</code> . |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To refresh the S-TAP details for the host 12.21.12.12:

```
grdapi refresh_stap_info stapHost=12.21.12.12
```

Typical response:

```
ID=0  
ok
```

Related reference

- [S-TAP and inspection engine APIs](#)

register_oauth_client

This API wraps supported GuardAPI functions in a REST API that uses JSON for input and output.

Note: The `register_oauth_client` API does not support the `redirect_uris` and `scope` parameters. These parameters are hard-coded for Guardium. If you make changes to `redirect_uris` or `scope`, the values are validated, but Guardium does not use them.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
register_oauth_client parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------|------------|--|
| client_id | String | Required. |
| GetToken | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| grant_types | String | For valid values, call register_oauth_client from the command line with --help=true. |
| password | String | The user password. |
| user | String | The username for the Guardium UI. |
| redirect_uris | String | Guardium does not support this parameter. Guardium suggests that you leave the redirect_uris parameter blank. If you must enter a value, the only valid value is https://someApp. |
| scope | String | Guardium does not support this parameter. Guardium suggests that you leave the scope parameter blank. If you must enter a value, you can enter one or more of the following comma-separated values, but Guardium ignores them: <ul style="list-style-type: none">• read• write• delete |

Example

```
grdapi register_oauth_client  
client_id=_home_markdown_jenkins_workspace_Transform_in_SSMPHH_12.x_com.ibm.guardium.doc.reference_grdapi_register_oauth_client_test12" grant_types="password" user="admin" password="password" GetToken=1
```

register_oauth_internal_client

This API manages the ROLE and USER for internal API requests.

For internal REST API requests, Guardium predefines a special ROLE and USER. This user cannot be removed or modified through the accessmgr UI and cannot be used to log in the UI. This user's password never expires, but is revoked if client ID is revoked.

On OAuth client registration, use this API to accept this user and client ID. The API generates and stores a random strong password for the user. The API then returns a client secret and the generated password. The internal (S-TAP, maybe others) client must secure the client secret and password.

To assign permissions for different functions, use the accessmgr UI.

This API is available in Guardium V10.1.4 and later.

GuardAPI syntax

```
register_oauth_internal_client parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------|------------|--|
| getEncrypted | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| grant_types | String | For valid values, call register_oauth_internal_client from the command line with --help=true. |
| module | String | Required. For valid values, call register_oauth_internal_client from the command line with --help=true. |
| redirect_uris | String | |
| scope | String | |

register_unit

REST API syntax

12.1 and later This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/register_unit
```

GuardAPI syntax

```
register_unit parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| secretKey | String | Required. |
| unitIp | String | Required. |
| unitPort | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

reinstall_policy

This command reinstalls the last uninstalled policy.

If you accidentally uninstall a policy, use this command to reinstall the policy.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/reinstall_policy
```

GuardAPI syntax

```
reinstall_policy parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| policy | String | Required. The name of the policy to reinstall. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi reinstall_policy policy="policy1"
```

Related reference

- [policy_uninstall](#)

reinstall_policy_rule

This command reinstalls one or more rules into a specified policy.

Specify multiple rules by using a pipe (|) character as a delimiter between rule names.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/reinstall_policy_rule
```

GuardAPI syntax

```
reinstall_policy_rule parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| policy | String | Required. The name of the policy. |
| ruleName | String | Required. The name of the rule or rules to reinstall. Use a pipe () character as a delimiter between rule names. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI examples

Uninstall a single policy rule:

```
grdapi reinstall_policy_rule policy="Hadoop Policy" ruleName="Low interest Objects: Allow"
```

Uninstall multiple policy rules:

```
grdapi reinstall_policy_rule policy="Hadoop Policy" ruleName="Low interest Objects: Allow|Low Interest Commands: Allow"
```

remove_all_from_schedule

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/remove_all_from_schedule
```

GuardAPI syntax

```
remove_all_from_schedule parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

remove_all_gr_replace_elements

This command deletes query replacement specifications from the system.

This API is available in Guardium V10.1.4 and later.

RestAPI syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/remove_all_gr_replace_elements
```

GuardAPI syntax

```
remove_all_gr_replace_elements parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|---|
| actionName | String | Required. A query rewrite action. |
| definitionName | String | Required. |
| replaceType | String | Specifies which replacement types are to be deleted. For valid values, call <code>remove_all_gr_replace_elements</code> from the command line with <code>--help=true</code> . |

Examples

```
grdapli remove_all_gr_replace_elements definitionName="new case 2" actionName="new qr action2"
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

remove_all_gr_replace_elements_byId

Deletes query replacement specifications from the system.

This API is available in Guardium V10.1.4 and later.

Rest API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/remove_all_gr_replace_elements_byId
```

GuardAPI syntax

```
remove_all_gr_replace_elements_byId parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|--|
| qrActionId | Long | Required. A query rewrite action identifier. |
| replaceType | String | Specifies which replacement types are to be deleted. If not specified, then all replacements for the specified action are deleted.
Valid values: <ul style="list-style-type: none">• SELECT• VERB• OBJECT• SENTENCE• SELECTLIST |

Examples

```
grdapi remove_all_gr_replace_elementsById qrActionName="qr_action15_2" replaceType="OBJECT"
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

remove_classifier_datasource

This command removes classification datasource.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/classifier_datasource
```

GuardAPI syntax

```
remove_classifier_datasource parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|-------------|
| datasourceName | String | Required. |
| processName | String | Required. |

remove_classifier_datasource_group

This command removes classification datasource groups.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/classifier_datasource_group
```

GuardAPI syntax

```
remove_classifier_datasource_group parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|-------------|
| groupName | String | Required. |
| processName | String | Required. |

remove_connection_properties

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/con_properties
```

GuardAPI syntax

```
remove_connection_properties parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| name | String | Required. |
| properties | String | |
| removeAll | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| type | String | Required. For valid values, call remove_connection_properties from the command line with --help=true. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

remove_custom_property_from_datasource_by_id

This API is available in Guardium V11.4 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/datasource_custom_prop_remove
```

GuardAPI syntax

```
remove_custom_property_from_datasource_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|-------------|
| customProps | String | Required. |
| id | Integer | Required. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

remove_custom_property_from_datasource_by_name

This API is available in Guardium V11.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/datasource_custom_prop_remove
```

GuardAPI syntax

```
remove_custom_property_from_datasource_by_name parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| customProps | String | Required. |
| name | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

remove_custom_property_from_datasources_in_group

This API is available in Guardium V11.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/datasource_group_custom_prop_remove
```

GuardAPI syntax

```
remove_custom_property_from_datasources_in_group parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|-------------|
| customProps | String | Required. |
| name | String | Required. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

remove_datasource_configuration_from_collector

This API is available in Guardium v12.0 and later.

GuardAPI syntax

```
remove_datasource_configuration_from_collector parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| ucDatasourceId | Integer | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

remove_datasource_from_entitlement_optimization

Removes the data of the specified datasources from the entitlement optimization data collection.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/removeDatasourceFromEntitlementOptimization
```

GuardAPI syntax

```
remove_datasource_from_entitlement_optimization parameter=value
```

| Parameter | Value type | Description |
|----------------|------------|-------------|
| datasourceName | String | Required. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Disable entitlement optimization for the datasource SSQLSERVER.

```
grdapi remove_datasource_from_entitlement_optimization datasourceName=SSQLSERVER
```

Related concepts

- [Entitlement optimization](#)

Related reference

- [Entitlement optimization APIs](#)

remove_datasource_from_group

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/datasource_group
```

GuardAPI syntax

```
remove_datasource_from_group parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|-------------|
| datasourceName | String | Required. |
| groupName | String | Required. |

remove_dm_from_profile

Removes the DM from the profile. If the profile is Active, running this command also unschedules the DM.

This API is available in Guardium V10.5 and later.

REST API syntax

This API is available as a REST service with the `DELETE` method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/datamartInProfile
```

GuardAPI syntax

```
remove_dm_from_profile parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------|------------|--|
| datamart_name | String | Required. The DM to delete from the profile. A datamart that belongs to the profile. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| profile_name | String | Required. The profile from which to delete the DM. For valid values, run <code>grdapi get_extraction_profile_info</code> or call <code>remove_dm_from_profile</code> from the command line with <code>--help=true</code> . |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • <code>all_managed</code>: execute on all managed units but not the central manager • <code>all</code>: execute on all managed units and the central manager • <code>group:<group name></code>: execute on all managed units identified by <code><group name></code> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Example

Remove the data mart **Export:Full SQL** from the user defined profile **sql_all**

```
remove_dm_from_profile profile_name=sql_all datamart_name=Export:Full SQL
```

Related concepts

- [Big Data Intelligence with data marts](#)

Related reference

- [Big Data Intelligence APIs](#)

remove_domain_from_universal_connector_allowed_domains

Run this API to remove authorization for communication with cloud-based database domains.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/removeDomainFromUcAllowedDomains
```

GuardAPI syntax

```
remove_domain_from_universal_connector_allowed_domains parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| domain | String | Required. The name of the domain to remove. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • <code>all_managed</code>: execute on all managed units but not the central manager • <code>all</code>: execute on all managed units and the central manager • <code>group:<group name></code>: execute on all managed units identified by <code><group name></code> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

To remove authorization for communication with [amazonaws.com](#):

```
grdapi remove_domain_from_universal_connector_allowed_domains domain=amazonaws.com
```

Related reference

- [Guardium universal connector APIs](#)

remove_extraction_profile

Removes an inactive, user-defined GBDI (Big Data) profile.

This API is available in Guardium V10.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/extractionProfile
```

GuardAPI syntax

```
remove_extraction_profile parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| profile_name | String | Required. The inactive profile you are removing. For valid values, run <code>grdapiget_extraction_profile_info</code> or call <code>remove_extraction_profile</code> from the command line with <code>--help=true</code> . |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To remove the profile `sql_all`:

```
remove_extraction_profile parameter=sql_all
```

Related concepts

- [Big Data Intelligence with data marts](#)

Related reference

- [Data mart APIs](#)

remove_members_of_groups_by_desc

Remove all members from a group identified by its description.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/remove_members_of_groups_by_desc
```

GuardAPI syntax

```
remove_members_of_groups_by_desc parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| desc | String | Required. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Example

Use this command to remove all the members from the group "group one":

```
grdapi remove_members_of_groups_by_desc desc="group one"
```

remove_members_of_groups_by_id

Remove all the member from a group identified by its identification key.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `DELETE` method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/remove_members_of_groups_by_id
```

GuardAPI syntax

```
remove_members_of_groups_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| id | Integer | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Example

Use this command to remove all the members from the group with identification key 100005:

```
grdapi remove_members_of_groups_by_id id=100005
```

remove_mfa_exempt_users

This command removes users from the exempt list for multi-factor authentication.

After a user is removed from the exempt list, Guardium will request secondary authentication to log in.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/configure_mfa
```

GuardAPI syntax

```
remove_mfa_exempt_users parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| exemptUsers | String | A comma-separated list of one or more users to remove from the list of exempt users. |
| mfaType | String | Required. The authentication type. For valid values, call remove_mfa_exempt_users from the command line with --help=true. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group: <group name>; execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapi remove_mfa_exempt_users exemptUsers="Hadrian,Fred" mfaType=DUO
```

Related concepts

- [Portal configuration](#)

Related reference

- [add_mfa_exempt_users](#)

remove_objects_native_audit

This API disables the object audit (audit trail) on the specified objects in the specified datasource.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/remove_objects_native_audit
```

GuardAPI syntax

```
remove_objects_native_audit parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| datasource_name | String | Required. A cloud datasource defined in Guardium. |
| objects | String | Required. A comma-separated list of objects. View objects with the get_native_audit_objects API or in the GUI. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related tasks

- [Cloud database service protection with native audit](#)

Related reference

- [Native audit APIs](#)

remove_populate_group_from_query

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/group_query
```

GuardAPI syntax

```
remove_populate_group_from_query parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| groupDesc | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

remove_qr_action

This command deletes a specified query rewrite action from the system.

This API is available in Guardium V10.1.4 and later.

Rest API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/qr_action
```

GuardAPI syntax

```
remove_qr_action parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|---------------------------------------|
| actionName | String | Required. A query rewrite action. |
| definitionName | String | Required. A query rewrite definition. |

Examples

```
grdapic remove_qr_action actionName="qr_action15_2" definitionName="case_15"
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

remove_qr_add_where_by_id

Deletes a specified "add where" function from the system.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/remove_qr_add_where_by_id
```

GuardAPI Syntax

```
remove_qr_add_where_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------|------------|------------------------------------|
| qrAddWhereId | Long | Required. An "add where" function. |

Examples

```
grdapic remove_qr_add_where_by_id qrAddWhereId=22666
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

remove_qr_condition

Deletes a query rewrite condition from the system.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/qr_condition
```

GuardAPI syntax

```
remove_qr_condition parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|---------------------------------------|
| conditionName | String | Required. A query rewrite condition. |
| definitionName | String | Required. A query rewrite definition. |

Examples

```
grdapic remove_qr_condition conditionName="qr_cond15_1" definitionName="case 15"
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

remove_qr_definition

This command removes a query rewrite condition.

This API is available in Guardium V10.1.4 and later.

REST API syntax

REST API: This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/qr_definition
```

Syntax

```
remove_qr_definition parameter=value
```

| Parameter | Value type | Description |
|----------------|------------|-------------|
| definitionName | String | Required. |

Examples

To remove the query rewrite definition "case 15":

```
grdapic remove_qr_definition definitionName="case 15"
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

remove_qr_replace_element_byId

Deletes a specified query element replacement, specified by ID, from the system.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/remove_qr_replace_element_byId
```

GuardAPI syntax

```
remove_qr_replace_element_byId parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------------|------------|--|
| qrReplaceElementId | Long | Required. A replacement definition ID. |

Examples

```
grdapi qrReplaceElementId=333333
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

remove_ranger_config

This command deletes the Ranger configuration for the specified cluster. All monitoring for these services is disabled upon restart of the affected Hadoop components.

This command requires valid administrative authority on the Ambari server such as an admin or service administrator account. After running the command, the Ambari administrator must restart the affected Hadoop components so that the changes take effect.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/remove_ranger_config
```

GuardAPI syntax

```
remove_ranger_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| clusterName | String | Name of the cluster. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> all_managed: execute on all managed units but not the central manager all: execute on all managed units and the central manager group:<group name>: execute on all managed units identified by <group name> host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

API examples

To delete the cluster named Cluster4:

```
grdapi remove_ranger_config clusterName=Cluster4
```

Sample output:

```
ID=0
The Hadoop service has been configured to disable monitoring. Ask the Hadoop administrator to restart the Hadoop services to
activate the changes
Configuration with ID: 2 deleted successfully
```

RestAPI example

```
curl -k --header "Authorization:Bearer ec4e55b5-79a9-4d02-9c5f-7a42672675a8" -i -H "Content-Type: application/json" -X DELETE -
d '{clusterName="hw3"}' https://<Guardium server name>:8443/restAPI/remove_ranger_config
```

Related concepts

- [Hadoop integration using Hortonworks and Apache Ranger](#)

Related reference

- [Hadoop monitoring APIs](#)
- [S-TAP Hadoop parameters](#)

remove_ranger_service

This command removes a ranger service from monitoring, from the specified cluster.

This command requires valid administrative authority on the Ambari server such as an admin or service administrator account. After running the command, the Ambari administrator must restart the affected Hadoop components so that the changes take effect.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/remove_ranger_service
```

GuardAPI syntax

```
remove_ranger_service parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| clusterName | String | Required. Ambari cluster name. |
| serviceName | String | Required. Name of the service. Valid values: <ul style="list-style-type: none">• hdfs• hive• hbase• kafka• solr• storm |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GrdAPI Example

To remove the ranger service HDFS, on the cluster named Cluster4:

```
grdapi remove_ranger_service clusterName=Cluster4 serviceName=HDFS
```

Sample output:

```
ID=0
Service: HDFS deleted successfully
```

RestAPI example

```
curl -k --header "Authorization:Bearer 27d21f39-0978-4c8f-9525-990876f092e0" -i -H "Content-Type: application/json" -X DELETE -d '{clusterName="hw3cl1"}' https://<guardium server>:8443/restAPI/remove_ranger_config
```

Related concepts

- [Hadoop integration using Hortonworks and Apache Ranger](#)

Related reference

- [Hadoop monitoring APIs](#)

- [S-TAP Hadoop parameters](#)

[remove_threshold_from_rule](#)

Use this API to remove a threshold from a violation policy rule that creates an active threat analytics case type.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/remove_threshold_from_rule
```

GuardAPI syntax

```
remove_threshold_from_rule parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|--|
| policy_name | String | Required. The policy that has the rule that you want to delete. Use the API <code>list_policy</code> to view policies. |
| rule_name | String | Required. The rule that you want to delete the threshold from. Use the API <code>list_policy_rules</code> to view rules. |

Examples

To remove the threshold from ruleNNN in policyAAA:

```
grdapli remove_threshold_from_rule policy_name=AAA rule_name=ruleNNN
```

Related tasks

- [Creating threat categories from policy rules](#)

Related reference

- [Policy and rule APIs](#)
- [Active threat analytics and risk spotter APIs](#)
- [list_policy_rules](#)
- [list_policy](#)

[replace_active_profile](#)

Changes the active profile of the GBDI (Big Data) interface, only if the interface is enabled.

This API is available in Guardium V10.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/extractionProfile
```

GuardAPI syntax

```
replace_active_profile parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------------|------------|---|
| new_active_profile | String | Required. An existing profile, which replaces the current profile. For valid values, run <code>grdapli get_extraction_profile_info</code> or call <code>replace_active_profile</code> from the command line with <code>--help=true</code> . Valid values: |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Change the active profile to `sql_all`.

```
new_active_profile profile_name=sql_all
```

Related concepts

- [Big Data Intelligence](#)

Related reference

- [Big Data Intelligence APIs](#)

reregister_agg_collector

Use this command to un-register a collector from its current aggregator, and register it with the specified aggregator.

This API is available in Guardium V10.1.4 and later.

GuardAPI syntax

```
reregister_agg_collector parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| newDomain | String | The domain name of the new host. |
| newHostName | String | Required. Aggregator you are registering the collector with. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To reregister the aggregator with the collector named coll44:

```
grdapic reregister_agg_collector newHostName=coll44
```

rerun_datamart

This command reruns a datamart for a period it already ran. It is useful if not all relevant data was available during the previous datamart run. For example, a datamart runs on an aggregator, but export data from one of the collectors hadn't been received in time.

This API is available in Guardium V11.0 and later.

GuardAPI syntax

```
rerun_datamart parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------|------------|---|
| datamartName | String | Required. |
| periodEnd | Date | Required. The end time of the period you are rerunning in the format: YYYY-MM-DD H24:MI:SS. |
| periodStart | Date | Required. The start time of the period you are rerunning in the format: YYYY-MM-DD H24:MI:SS. |

Examples

To rerun the data mart Export:Full SQL:

```
grdapi rerun_datamart datamartName="Export:Full SQL" periodStart="2019-08-01 00:00:00" periodEnd="2019-08-01 23:59:59"
```

Related concepts

- [Data mart](#)

Related reference

- [Data mart APIs](#)

rerun_distributed_report

Use this API to manually rerun a distributed report, typically used if the automatic run results were not complete.

For example, a distributed report runs daily at 1AM, and it collects data from aggregators. Data from one of the collectors was not received before the previous run of the report. To get a complete report, you need to verify that all data is in the aggregator; delete the results of this incomplete run (with the API [delete_distributed_report_result_for_period](#)); and rerun the distributed report manually for this period.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
rerun_distributed_report parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|--|
| endTime | Date | Required. |
| hostname | String | Required. |
| reportId | Integer | Required. |
| runOptions | String | Required. Valid values: <ul style="list-style-type: none">• <i>forHostname</i>• <i>forAllFailed</i>• <i>forceRerunForHostname</i>• <i>forceRerunForAllUnits</i> |
| startTime | Date | Required. |

Related concepts

- [Distributed report builder](#)

Related reference

- [Reports and report generation APIs](#)

reset_unit_utilization_data

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/reset_unit_utilization_data
```

GuardAPI syntax

```
reset_unit_utilization_data parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| hostName | String | Required. |
| resetDate | Date | Required. |

reset_va_summary_by_id

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/reset_va_summary_by_id
```

GuardAPI syntax

```
reset_va_summary_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|-------------|
| resetCumulativeFailTo | Integer | |
| resetCumulativePassTo | Integer | |
| summaryId | Integer | Required. |

reset_va_summary_by_key

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/reset_va_summary_by_key
```

GuardAPI syntax

```
reset_va_summary_by_key parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|-------------|
| datasourceName | String | Required. |
| hostName | String | Required. |
| port | Integer | Required. |
| resetCumulativeFailTo | Integer | |
| resetCumulativePassTo | Integer | |
| serviceName | String | Required. |

rest_export_definition

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available only as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/export_definition
```

Parameters

| Parameter | Value type | Description |
|---------------------|------------|--|
| dataSet | String | Required. For valid values, call rest_export_definition from the command line with --help=true. |
| itemNames | String | |
| exportToCSV | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| exportToXacml | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| excludeGroupMembers | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |

restart_all_managed_units

Run this command on a central manager to restart the GUIs on all of its managed units.

This API is available in Guardium V10.6 and later.

GuardAPI syntax

```
restart_all_managed_units parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To restart the GUIs of all of the managed units of the central manager, enter on the central manager:

```
grdapic restart_all_managed_units
```

restart_cloud_instance

Restarts the specified cloud instance (defined for cloud database service protection).

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/restart_cloud_instance
```

GuardAPI syntax

```
restart_cloud_instance parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| datasource_name | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapi
```

restart_job_queue_listener

This command restarts the job queue listener. Run this command if the job queue fails to start, does not run waiting jobs, or if a job appears stuck in running or stopping status.

Calling this command immediately restarts the job queue, and any currently running jobs are halted and restarted.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/restart_job_queue_listener
```

GuardAPI syntax

```
restart_job_queue_listener parameter=value
```

This API takes no parameters.

GuardAPI example

```
grdapi restart_job_queue_listener
```

restart_solv

This command restarts the solv process on the specified Guardium® system(s).

This API is available in Guardium V10.6 and later.

GuardAPI syntax

```
restart_solv parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|--|
| restart_all | Boolean | <p>This parameter is only relevant when running the command on a CM. Valid values:</p> <ul style="list-style-type: none">• 0 (false): solv is restarted only on CM• 1 (true): solv is restarted on CM and all managed units. <p>Default = 0 (false)</p> |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapi restart_solr restart_all=true
```

Related reference

- [Solr APIs](#)

restart_stap

This command restarts the S-TAP on the specified database server.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/stap
```

GuardAPI syntax

```
restart_stap parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| restartMode | Integer | <p>Controls the S-TAP behavior when it receives a restart command. Valid values:</p> <ul style="list-style-type: none"> • 0: Restarts the S-TAP • 1: Requests new collectors from the central manager (enterprise load balancer), and does not restart the S-TAP <p>Default = 0</p> |
| stapHost | String | Required. Hostname |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To restart the S-TAP® on the database server with the IP address 9.42.29.158:

```
grdapi restart_stap stapHost=9.42.29.158
```

Related reference

- [S-TAP and inspection engine APIs](#)

restart_unit_pinger

This API restarts the internal UnitPinger thread.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
restart_unit_pinger parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related reference

- [get_unit_pinger](#)

restore_units_after_bad_shift

Run this command if, after a switch to a backup central manager, some or all of the managed units are not registered with the new primary central manager.

This API is available in Guardium V11.0 and later.

GuardAPI syntax

```
restore_units_after_bad_shift parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

retrieveUpdatedUsers

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/retrieveUpdatedUsers
```

GuardAPI syntax

```
retrieveUpdatedUsers parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|-------------|
| dcName | String | Required. |
| lastUpdateTime | String | Required. |

retrieveAPIs

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available only as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/restapi
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|--|
| withParameters | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| apiNameLike | String | |

retrieveApiParameters

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available only as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/restapi
```

Parameters

| Parameter | Value type | Description |
|------------|------------|-------------|
| resourceId | Integer | |

revokeOAuthClient

This API revokes access to the REST APIs for a specified client.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/revokeClient
```

GuardAPI syntax

```
revokeOAuthClient parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| | | |

| Parameter | Value type | Description |
|-----------------|------------|---|
| client_id | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

revokeOAuthToken

This API revokes a specified REST API token.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
revokeOAuthToken parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| token | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

revoke_api_key

12.1 and later This command deletes an API key for a Guardium user.

GuardAPI syntax

```
delete_api_key parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| name | String | Required. |
| username | String | If not specified, deletes the API key for the logged-in user. If specified, the logged-in user must have the accessmgr role to delete the API key for the user associated with the username. |

GuardAPI example

The following example shows the command to delete the API key `VAScanner_IT` for the `guard` user.

```
grdapi revoke_api_key name=VAScanner_IT username=guard
```

revoke_ignore_stap

This command revokes existing IGNORE S-TAP SESSION (REVOKABLE) policy rule actions that ignore S-TAP® session traffic. This command only revokes soft ignore rules (marked as REVOKABLE) and cannot revoke hard rules (not marked as REVOKABLE).

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/revoke_ignore_stap
```

GuardAPI syntax

```
revoke_ignore_stap parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| stapHost | String | For valid values, call <code>revoke_ignore_stap</code> from the command line with <code>--help=true</code> . |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapi revoke_ignore_stap
```

Related concepts

- [Policy rule actions](#)

Related reference

- [S-TAP and inspection engine APIs](#)

revoke_role_from_object_by_Name

Removes a role from the specified object.

Guardium automatically handles dependencies. For example, if you remove role `accessmgr` from a specific query, role `accessmgr` is also removed from any report based on that query.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `DELETE` method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/revoke_role_from_object_by_Name
```

GuardAPI syntax

```
revoke_role_from_object_by_Name parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|--|
| objectName | String | Required. The name of the object from which to revoke the role. |
| objectType | String | Required. The name of the object type. For valid values, call <code>revoke_role_from_object_by_Name</code> from the command line with <code>--help=true</code> . |
| role | String | Required. The name of the role to revoke. Specify any existing role. Specify <code>all_roles</code> to remove access to all roles. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi revoke_role_from_object_by_Name objectType=Datasource objectName="swanSybase" role=admin
```

revoke_role_from_object_by_id

Removes a role from the specified object.

Guardium automatically handles dependencies. For example, if you remove role 7 from a specific query, role 7 is also removed from any report based on that query.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/revoke_role_from_object_by_id
```

GuardAPI syntax

```
revoke_role_from_object_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| objectId | Integer | Required. The ID of the object from which to revoke the role. |
| objectTypeId | Integer | Required. The ID of the object type. For valid values, call <code>revoke_role_from_object_by_id</code> from the command line with <code>--help=true</code> . |
| roleId | Integer | Required. The ID of the role to revoke from the object. Specify any existing role ID or specify -1 to revoke access to all roles. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi revoke_role_from_object_by_id objectId=13 objectTypeId=13 roleId=-1
```

Related reference

- [grant_role_to_object_by_id](#)

riskspotter_set_config

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/riskspotter_set_config
```

GuardAPI syntax

```
riskspotter_set_config parameter=value
```

This API takes no parameters.

rule_info_from_policy

This command displays information about all of the rules that make up a specified policy.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/ruleInfoFromPolicy
```

GuardAPI syntax

```
rule_info_from_policy parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| localeLanguage | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| policyDesc | String | Required. The name of the policy. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

GuardAPI example:

```
> grdapi rule_info_from_policy policyDesc="Copy of Basel II [template]"
```

REST API example:

```
curl -k --header "Authorization:Bearer 57c9bcc5-b7af-441b-a836-94d72c28174c" -i -H "Content-Type: application/json" -X GET  
"https://example.com:8443/restAPI/ruleInfoFromPolicy/?policyDesc=testPol"
```

run_custom_table_ldap_import

This command imports LDAP data into a custom table.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/custom_data_ldap
```

GuardAPI syntax

```
run_custom_table_ldap_import parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| importId | Integer | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

run_database_instance_discovery

This API is available in Guardium v10.1.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/run_database_instance_discovery
```

GuardAPI syntax

```
run_database_instance_discovery parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------------|------------|---|
| replaceInspecti
onEngine | Boolean | <p>Valid values:</p> <ul style="list-style-type: none">• 0 (false)• 1 (true) <p>Default = 0 (false)</p> |
| stapHost | String | Required. For valid values, call <code>run_database_instance_discovery</code> from the command line with <code>--help=true</code> . |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

run_diagnostics

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/run_diagnostics
```

GuardAPI syntax

```
run_diagnostics parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| durationInSec | Integer | |
| level | Integer | |
| stapHost | String | Required. For valid values, call run_diagnostics from the command line with --help=true. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

run_populate_group_from_query

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/group_query
```

GuardAPI syntax

```
run_populate_group_from_query parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| groupDesc | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

run_universal_connector

Enables the Guardium universal connector on the local or specified collectors.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/runUniversalConnector
```

GuardAPI syntax

```
run_universal_connector parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------------|------------|--|
| enable_metrics | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| overwrite_old_instance | Boolean | Determines whether to overwrite the container (erase all saved data and restart the Guardium universal connector).Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| uc_debug_level | String | Valid values: <ul style="list-style-type: none">• <i>all</i>• <i>debug</i>• <i>info</i>• <i>warn</i>• <i>error</i>• <i>fatal</i>• <i>off</i>• <i>trace</i> |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• <i>all_managed</i>: execute on all managed units but not the central manager• <i>all</i>: execute on all managed units and the central manager• <i>group:<group name></i>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To start the Guardium universal connector on your local Guardium system:

```
grdapi run_universal_connector
ID=0
Universal-Connector container was started
ok
```

Related concepts

- [Guardium universal connector](#)

Related reference

- [Guardium universal connector APIs](#)

sched_cust_table_distribution

This API schedules the distribution of custom tables.

This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/custTblDist
```

GuardAPI syntax

```
sched_cust_table_distribution parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| cronString | String | Required. The schedule to distribute the table as a cron string. For example, to run the job every day at 2 AM:

0 2 * * * |
| customTableName | String | Required. The name of the custom table to distribute. |
| startTime | Date | The time to start running the distribution job, in the format yyyy-mm-dd hh:mm:ss. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> all_managed: execute on all managed units but not the central manager all: execute on all managed units and the central manager group:<group name>: execute on all managed units identified by <group name> host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123. host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related tasks

- [Distribute custom tables](#)

Related reference

- [delete_cust_table_distribution_schedule](#)

schedule_generate_mongo_filter_job

This API defines the lists of groups IDs of the users, objects, and commands that are used to create a Guardium universal connector filter for MongoDB.

The groups in this API are used to continuously update the value of the GIM parameter GUC_AUDIT_LOG_FILTER. The GIM parameter specifies which events to include in the data forwarded to the Guardium universal connector.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/scheduleGenerateMongoFilterJob
```

GuardAPI syntax

```
schedule_generate_mongo_filter_job parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|---|
| clientIp | String | The IP of the GIM client whose GIM parameter GUC_AUDIT_LOG_FILTER gets updated. |
| commandGroupId | String | String of comma separated IDs of groups whose members specify tuples of DB name and command to be included in the native log audit that is forwarded to the Guardium universal connector. If this parameter is not required for the filter, use <code>usersGroupId=""</code> . |
| cronStr | String | Optional. Cron string that defines when to run the code that updates the filter in the GIM parameter GUC_AUDIT_LOG_FILTER. Default is every night at 00:15: "0 15 0 * * ? *" |
| objectsGroupId | String | String of comma separated IDs of groups whose members specify the tuples of DB name and collection to be included in the native log audit that is forwarded to the Guardium universal connector. If this parameter is not required for the filter, use <code>usersGroupId=""</code> . |
| startTime | Date | When to start the scheduling.
Default: now (null) |
| usersGroupId | String | String of comma separated IDs of groups whose members specify the tuples of DB Name and user name to be included in the native log audit that is forwarded to the Guardium universal connector. If this parameter is not required for the filter, use <code>usersGroupId=""</code> . |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapi schedule_generate_mongo_filter_job clientIp="9.42.135.95" usersGroupId="20000,20001" objectsGroupId="20004,20005"
commandGroupId="20002,20003"
```

Related concepts

- [Guardium universal connector](#)

Related reference

- [Guardium universal connector APIs](#)

schedule_job

This API schedules a specified job type to run at a specific time.

Note: Some job types do not require an object name. No validation is performed on the object name parameter for the following job types. When you run the API with anything entered as the objectName parameter, the standard 'OK' prompt is returned:

- AppUserTranslation
- CSVExport
- DataArchive
- DataExport
- DataImport
- InstallPolicy
- IpHostToAlias
- ResultsArchive
- SystemBackup

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/schedule_job
```

GuardAPI syntax

```
schedule_job parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|--|
| cronString | String | Required. |
| jobType | String | Required. For valid values, call <code>schedule_job</code> from the command line with <code>--help=true</code> . |
| objectName | String | |
| startTime | Date | |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

search

This REST API is a wrapper for Solr queries, which are used in the Investigation Dashboard.

Note: The [quick_search](#) REST API provides similar capabilities to this command, but provides more flexibility.

Note: The search API returns codes that represent the titles of the columns (fields) in the returned tables. For example, search might return the following rows:

```
"15": "Failed Login - Alert and Quarantine if Repeated",
"16": "5",
```

To map the codes ("15" and "16", in this case) to the actual column names, use the [getFieldsTitles](#) API.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available only as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/search
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| CATEGORY | String | The Guardium Solr collections. The categories generally map to the categories that are shown in the Investigation dashboard UI. For valid values, call search from the command line with <code>--help=true</code> . |
| COUNT | Integer | The number of records to return.
Default = 50. |
| END_TIME | String | Search for records that were created before the specified END_TIME. The time must be specified in the format: <code>YYYYMMDD+HH:MM:SS</code> . |
| QUERY | String | A Solr query. |
| START | Integer | The record on which to start searching.
Default = 0. |
| START_TIME | String | Search for records that were created after the specified START_TIME. The time must be specified in the format: <code>YYYYMMDD+HH:MM:SS</code> . |
| SUMMARY_BY | String | Group results by the selected field code. You can specify up to 2 field title codes to group by.
Note: To map the field codes to column names, use the getFieldsTitles API. |
| WITH_FACETS | String | <p>Include facets in the search. For more information, see Investigation dashboard for data or Investigation dashboard for files. Valid values are:</p> <ul style="list-style-type: none"> • 0 (Off: Do not include facets) • 1 (On: Include facets) <p>Default = 0.</p> |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Use the START and COUNT parameters to specify the starting record and the number of records to return. The following example returns 20 records from the Violation category, starting with the 10th record:

```
curl -k --header "Authorization: Bearer 3499f352-aa98-4046-89d8-aba3d8c12345"
"https://xxx.xxx.xxx:8443/restAPI/search?CATEGORY=VIOLATION
&START_TIME=20190115+03:59:00&END_TIME=20190215+15:39:39&START=10&COUNT=20"
```

Returns the following information.

```
{
  "totalHits": 5,
  "numRows": 5,
  "partialResults": false,
  "count": 5,
  "start": 0,
  "maxLengthMapByOrder": [
    {
      "6": -1
    },
    {
      "10": -1
    },
    {
      "7": -1
    },
    {
      "4": -1
    },
    {
      "2": -1
    },
    ...
  ],
  "items": [
    {
      "15": "Failed Login - Alert and Quarantine if Repeated",
      "16": "5",
      "13": "",
      "id": "0",
      "3": "10.10.9.56",
      "2": "JOAN",
      "1": "ORACLE",
      ...
    },
    {
      "15": "Privileged Users Access to Sensitive Objects -- TERMINATE",
      "16": "10",
      "13": "select * from joe.creditcard",
      "id": "1",
      "3": "10.10.9.56",
      "2": "RODRIGO",
      "1": "ORACLE",
      ...
    },
    {
      "15": "DML on SOX Financial Objects -- Terminate",
      "16": "10",
      "13": "insert into creditcard (custid",
      "id": "2",
      "3": "10.10.9.56",
      "2": "CASSANDRA",
      "1": "",
      ...
    },
    {
      "15": "Privileged Users Access to Sensitive Objects -- TERMINATE",
      "16": "10",
      "13": "select * from db2inst1.US_CUST",
      "id": "3",
      "3": "10.10.9.56",
      "2": "DB2INST1",
      "1": "DB2INST1",
      ...
    },
    {
      "15": "Privileged Users Access to Sensitive Objects -- TERMINATE",
      "16": "10",
      "13": "select * from joe.ssn",
      "id": "4",
      "3": "10.10.9.56",
      "2": "SYSTEM",
      "1": "ORACLE",
      ...
    }
  ],
  "facets": [],
  "searchArgs": {
    "start": 0,
    "count": 50,
    "isFam": false,
    "isFamGUI": false,
    "withFacets": false,
    "category": "VIOLATION",
    "startTime": "20190115 03:59:00",
    "endTime": "20190215 15:39:39",
    ...
  }
}
```

```

        "intStartTime": 1445988306,
        "intEndTime": 1484512779,
        "maxResultsNum": 50,
        "summaryTotalsOnly": false,
        "partialSummary": false,
        "timeResolution": {
            "units": 0,
            "scale": "NA",
            "difference": 0
        },
        "summarySortedBy": "COUNT",
        "localSearch": false,
        "fullSearch": false,
        "changeDashboardSettings": false,
        "sortOrder": "desc"
    },
    "searchSolr": false
}
]

```

Related concepts

- [Investigation Dashboard](#)

Related reference

- [getFieldsTitles](#)
- [quick_search](#)

secure_settings

12.1 and later This API command is used to manage the security commands in Guardium.

REST API syntax

This API is available as a REST service with the **secureSettings** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/secure_settings
```

GuardAPI syntax

```
secure_settings parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| component | String | Valid values are: <ul style="list-style-type: none"> • <i>sshd</i> • <i>ciphers</i> • <i>services</i> |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> • <i>all_managed</i>: execute on all managed units but not the central manager • <i>all</i>: execute on all managed units and the central manager • <i>group:<group name></i>: execute on all managed units identified by <i><group name></i> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <i>api_target_host=10.0.1.123</i>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <i>api_target_host=10.0.1.123</i>.
IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Secure settings for ssh

| Parameter | Value type | Description |
|-----------|------------|-------------|
| | | |

| Parameter | Value type | Description |
|-----------|------------|--|
| show | String | Valid values are: <ul style="list-style-type: none">• <i>all</i>• <i>dsa_state</i>• <i>max_connection</i>• <i>port_number</i>• <i>secure_state</i>• <i>ssh_key_mode</i>• <i>ssh_match_address</i>• <i>version</i> |
| store | String | Valid values are: <ul style="list-style-type: none">• <i>dsa_state</i>• <i>max_connection</i>• <i>port_number</i>• <i>secure_state</i>• <i>ssh_key_mode</i>• <i>ssh_match_address</i> |
| value | String | Options are: <ul style="list-style-type: none">• <i>on</i>• <i>off</i>• <i>secure</i>• <i>default</i>• <number>• <address_expression> |

Secure settings for ciphers

| Parameter | Value type | Description |
|-----------|------------|--|
| type | String | Valid values are: <ul style="list-style-type: none">• <i>java</i>• <i>inspection_core</i> |
| delete | String | Valid value is: <ul style="list-style-type: none">• <cipher_list> |
| disable | String | Valid values are: <ul style="list-style-type: none">• <ciphers> |
| enable | String | Valid values are: <ul style="list-style-type: none">• <i>default</i>• <i>cbc</i>• <i>dhe</i>• <i>cipherlist</i> |
| show | String | Valid values are: <ul style="list-style-type: none">• <i>current</i>• <i>disabled</i> |
| show_like | String | Valid value is: <ul style="list-style-type: none">• <pattern> |
| store | String | Valid values are: <ul style="list-style-type: none">• <i>default</i>• <i>cipherlist</i> |

Secure settings for services

| Parameter | Value type | Description |
|-----------|------------|---|
| disable | String | Valid value is: <ul style="list-style-type: none">• <servicename> |
| enable | String | Valid value is: <ul style="list-style-type: none">• <servicename> |
| status | String | Valid value is: <ul style="list-style-type: none">• <servicename> |

Examples

The following command lists the secure settings.

```
grdapi secure_settings  
ID=0  
Usage: grdapi secure_settings component={sshd|ciphers|services}  
arguments as necessary for the components
```

The following command is used to manage the ssh daemon sshd component.

```
grdapi secure_settings component=sshd <options>  
options:  
  show=all  
  show=dsa_state  
  show=max_connection  
  show=port_number  
  show=secure_state  
  show=ssh_key_mode  
  show=ssh_match_address  
  show=version  
  
  store=dsa_state value={on|off}  
  store=max_connection value=<number>  
  store=port_number value=<number>  
  store=secure_state value={secure|default}  
  store=ssh_key_mode value={on|off}  
  store=ssh_match_address value=<address_expression>
```

The following command is used to manage the ciphers component.

```
grdapi secure_settings component=ciphers <options>  
options:  
  type=java show={current|disabled}  
  type=java show_like=<pattern>  
  type=java disable=<ciphers>  
  type=java enable={cbc|dhe|cipherlist}  
  
  type=inspection_core show={default|all|current}  
  type=inspection_core show_like=<pattern>  
  type=inspection_core store={default|cipherlist}  
  type=inspection_core delete=<cipherlist>
```

The following command is used to manage the services component.

```
grdapi secure_settings component=services  
  
usage:  
grdapi secure_settings component=services status=<service>  
grdapi secure_settings component=services enable=<service>  
grdapi secure_settings component=services disable=<service>  
  
Possible services to view status:  
  all  
  cas (16019)  
  classifier  
  docker  
  gin (8446)  
  guard-insights (8586)  
  guard-snifbufusage  
  gui  
  jproxyforwarder  
  jproxystimer.timer  
  nanny  
  patch_installer  
  readahead-disable-services  
  sniffer  
  snmpd  
  sonarjproxyd  
  stap_upload (8444)  
These services can be enabled/disabled:  
  cas (16019)  
  docker  
  gin (8446)  
  guard-insights (8586)  
  guard-snifbufusage  
  patch_installer  
  snmpd  
  stap_upload (8444)
```

session_inference_control

Use the session_inference_control command to start or stop Session Inference.

Use session_inference_control to start or stop Session Inference from the command line. For more information, see [Session Inference control](#).

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/session_inference
```

GuardAPI syntax

```
session_inference_control parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| action | String | Required. Action can be: <ul style="list-style-type: none">• start: Start the session inference servlet.• stop: Stop the session inference servlet. |
| api_target_host | String | Required for GRD API. For REST APIs, this parameter is optional. If not specified for a REST API, defaults to the localhost.

Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>.
IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To start Session Inference from the command line with a GuardAPI:

```
test.swg.usma.ibm.com> grdapic session_inference_control action=start api_target_host=127.0.0.1
```

Related concepts

- [Session Inference](#)

Related reference

- [session_inference_setup](#)

session_inference_setup

Use the `session_inference_setup` command to configure Session Inference from the Guardium command line.

The `session_inference_setup` command provides a method of changing the Session Inference parameters from the command line. You can also set these parameters from the Guardium UI. Browse to `Setup > Tools and views > Session Inference`.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/session_inference
```

GuardAPI syntax

```
session_inference_setup parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------|------------|--|
| activeOnStartup | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Determines whether Session Inference starts automatically when the GUI starts |
| maxInactivePeriod | Integer | Number of minutes of inactivity before a session is marked as closed. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| pollingInterval | Integer | Frequency (in minutes) with which Session Inference checks for open sessions. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related concepts

- [Session Inference](#)

Related reference

- [session_inference_control](#)

setOAuthTokenExpirationTime

This API sets the expiration time of the REST API token.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
setOAuthTokenExpirationTime parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| expirationTime | Long | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapic setOAuthTokenExpirationTime ExpirationTime=10000
```

Related reference

- [getOAuthTokenExpirationTime](#)

set_alerter_settings

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/alerter_settings
```

GuardAPI syntax

```
set_alerter_settings parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| activeOnStartup | Boolean | Required. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| pollingInterval | Integer | Required. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

set_alerter_smtp_settings

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/alerter_smtp
```

GuardAPI syntax

```
set_alerter_smtp_settings parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| hostName | String | Required. |
| password | String | |
| port | Integer | Required. |
| returnPathEmail | String | Required. |
| starttls | String | Valid values: <ul style="list-style-type: none">• TLS• SSL• NONE |
| userName | String | |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

set_alerter_snmp_settings

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/alertersnmp
```

GuardAPI syntax

```
set_alerter_snmp_settings parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------------------|------------|---|
| hostName | String | Required. |
| secondaryHostN
ame | String | |
| secondaryTrapC
ommunity | String | |
| trapCommunity | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

set_certificate_host_validation

Enable this API to ensure that the central manager verifies that the SSL certificates contain a valid host name for all of its managed units.

When enabled, the central manager verifies that the SSL certificates contain a valid host name for all of the managed units. The default setting is `0` (false).

To ensure that all managed units have a valid SSL Certificate for the GUI, create a CSR and obtain a valid SSL certificate. Valid SSL certificates can also be obtained by using the `create self-signed gui` CLI command.

For more information about `create self-signed gui`, see [Certificate CLI Commands](#)

Note: If `set_certificate_host_validation` is enabled on a central manager when a managed unit has an invalid SSL Certificate, the communication between the central manager and managed unit fails.

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/setHostValidation
```

GuardAPI syntax

```
set_certificate_host_validation parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| enable | Boolean | Required. Valid values: <ul style="list-style-type: none">• <code>0</code> (false) - Default.• <code>1</code> (true) |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

set_debug_level

This command controls IMS output.

Note: If you set the IMS debug_level = 1, IMS debug fields such as mvs_is_plex, mvs_ipaddr, mvs_dlta_sign, and mvs_dlta_val are output to internal database tables, GDM_CONSTRUCT_TEXT.FULL_SQL, or GDM_EXCEPTION.FULL_SQL.

This API is available in Guardium® V9.5 and later.

GuardAPI syntax

```
set_debug_level parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| component | String | Required. Valid values: <ul style="list-style-type: none"> • <i>IMS</i>: IBM IMS • <i>DS_MSG</i>: Datasource message |
| level | Integer | Required. The debug level for this component. Valid values: <ul style="list-style-type: none"> • 0: Debug is off. • 1: Debug is on. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Example

To turn on debug for IMS:

```
grdapi set_debug_level component=IMS level=1
```

Sample output

```
This api will restart sniffer, please wait.
ID=0
ok
```

Related reference

- [get_debug_level](#)

set_distributed_report_target

Use this API to define a Guardium system as a target for distributed reports. After you define it here, it appears in the GUI as a defined target.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
set_distributed_report_target parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|--|
| target_host_name | String | Required. Hostname of the Guardium system. |

Examples

To define the Guardium system with the IP 11.11.11.11 as a target for distributed reports:

```
grdapic set_distributed_report_target target_host_name=11.11.11.11
```

Related concepts

- [Distributed report builder](#)

Related reference

- [Reports and report generation APIs](#)

set_enterprise_search_options

Use this command to specify which data is included in the investigation dashboard: data from all managed units in a centrally managed system, or an individual Guardium system. By default, a collector dashboard shows data from that collector, and the Central Manager dashboard shows data of the entire cluster.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
set_enterprise_search_options parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------------|------------|---|
| distributed_search | String | Required. Controls the sources of data that is displayed in the investigation dashboard. Valid values: <ul style="list-style-type: none"><i>cm_only</i>: Use this option on a central manager to retrieve data from all managed units in the centrally managed environment that have enable_quick_search=1. (If you enter <i>cm_only</i> on a managed unit, only data from that managed unit is displayed.)<i>all_machines</i>: Use this option on a managed unit in a centrally managed environment to include data from all units in the environment. <i>all_machines</i> mode requires open network access on port 8983 between all nodes, which might not comply with your security policies. Data retrieval might be slower than on the central manager. Default = <i>cm_only</i> |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"><i>all_managed</i>: execute on all managed units but not the central manager<i>all</i>: execute on all managed units and the central manager<i>group:<group name></i>: execute on all managed units identified by <i><group name></i>host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To configure the investigation dashboard to search data across the entire Guardium environment, from any Guardium system in that environment:

```
grdapic set_enterprise_search_options distributed_search=all_machines
```

Related concepts

- [Investigation dashboard](#)

Related reference

- [Investigation dashboard APIs](#)

set_entitlement_datasource_parameter

Modifies the configuration for a data source that is already enabled for entitlement optimization.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/setEntitlementDatasourceParameter
```

GuardAPI syntax

```
set_entitlement_datasource_parameter parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| datasourceName | String | Required. |
| parameterName | String | Required. Valid values: <ul style="list-style-type: none">• <code>isEnabled</code>• <code>userScore</code>• <code>objectScore</code>• <code>extractActivity</code>• <code>extractEntitlement</code>• <code>generateRoleClusters</code>• <code>generateNews</code>• <code>generateRecommendations</code>• <code>filterTempObjects</code>• <code>filterIgnoreVerbs</code> |
| parameterValue | String | Required. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

Enabled data from this datasource to the Recommendations tab.

```
grdapi set_entitlement_datasource_parameter datasourceName=SSQLSERVER extractEntitlement=1 generateRecommendations=1
```

Related concepts

- [Entitlement optimization](#)

Related reference

- [Entitlement optimization APIs](#)

set_expiration_date_for_restored_day

This command overwrites the expiration date for data that has been restored, specified by the date of the restored data, on one or more Guardium® systems. The original expiration date is defined in the restore operation (the parameter Don't purge restored data for at least).

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/expiration_date_for_restored_day
```

GuardAPI syntax

```
set_expiration_date_for_restored_day parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| newExpDate | String | Required. The new expiration date for the restored data. The format is one of: real day <code>yyyy-mm-dd hh:mi:ss</code> ; or relative day such as <code>NOW -10 day</code> . |
| restoredDay | String | Required. Identifies the day whose data was restored. The format is one of: real day <code>yyyy-mm-dd hh:mi:ss</code> ; or relative day such as <code>NOW -10 day</code> . |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

This command sets the expiration date for restored data that was collected 10 days ago, to 10 days from now:

```
grdapi set_expiration_date_for_restored_day newExpDate=NOW +10 day restoredDay=NOW -10 day
```

Related tasks

- [Managing stored data](#)

Related reference

- [Archive, export, import, purge, and restore APIs](#)

set_flatLogProcessType

This command sets the behavior of the flat log file.

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/flatLogProcessType
```

GuardAPI syntax

```
set_flatLogProcessType parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|--|
| processType | String | <p>Required. The type and action for this log file. The options are:</p> <ul style="list-style-type: none"> • ARCHIVE_AGGREGATE_PURGE: Archive or aggregate, and optionally purge, the flat log. • DEFAULT: No options are selected. • PROCESS : Merge the flat log information to the internal database. • PURGE_ONLY: Purge the flat log data. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi set_flatLogProcessType processType="PROCESS"
```

Related concepts

- [Flat Log Process](#)

set_health_traffic_job_interval

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/traffic_health_job
```

GuardAPI syntax

```
set_health_traffic_job_interval parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| interval | Integer | Required. |

set_import

Use this command to start or stop the import of data from an aggregator to one or more Guardium® collectors.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/set_import
```

GuardAPI syntax

```
set_import parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| | | |

| Parameter | Value type | Description |
|-----------------|------------|---|
| state | String | Required. Starts or stops the import of aggregator data to the collector. Valid values: <ul style="list-style-type: none"> • START • STOP |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

This command starts the import process:

```
grdapi set_import state=start
```

Related tasks

- [Managing stored data](#)

Related reference

- [Archive, export, import, purge, and restore APIs](#)

set_inapplicable_test_result_status

This API is available in Guardium v11.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/inapplicable_test_result_status
```

GuardAPI syntax

```
set_inapplicable_test_result_status parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------|------------|--|
| includeScore | Boolean | Required. Valid values: <ul style="list-style-type: none"> • 0 (false) • 1 (true) Default = 1 (true) |

set_ip_to_alias_overwrites

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/ip_to_alias_overwrites
```

GuardAPI syntax

```
set_ip_to_alias_overwrites parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------------|------------|---|
| ipToAliasOverwrites | Boolean | Required. Valid values: <ul style="list-style-type: none"> 0 (false) 1 (true) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> all_managed: execute on all managed units but not the central manager all: execute on all managed units and the central manager group:<group name>: execute on all managed units identified by <group name> host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

set_ip_to_alias_selected

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/ip_to_alias_selected
```

GuardAPI syntax

```
set_ip_to_alias_selected parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------|------------|---|
| ipToAliasSelected | Boolean | Required. Valid values: <ul style="list-style-type: none"> 0 (false) 1 (true) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> all_managed: execute on all managed units but not the central manager all: execute on all managed units and the central manager group:<group name>: execute on all managed units identified by <group name> host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

set_job_process_concurrency_limit

This command sets the job process concurrency limit.

Guardium can run multiple threads in parallel to optimize the performance and utilization of the CPU. To take advantage of this multi-threading feature, use the `set_job_process_concurrency_limit` command. This command defines the number of assessment and classifier processes that can run concurrently.

This API is available in Guardium V10.6 and later.

GuardAPI syntax

```
set_job_process_concurrency_limit parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| limit | Integer | <p>Required.</p> <p>The limit value defines the number of assessment and classifier processes that can run concurrently. The limit value is the lesser of 100 or twice the number of CPU cores installed on the Guardium system.</p> <p>For example, if a system has 8 CPU cores, the maximum limit value is 16. If a system has 64 CPU cores, the maximum limit value is 100.</p> <p>The default limit value is 1.</p> |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapi set_job_process_concurrency_limit limit=10
```

set_ktap_debug

Add a short description here.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/stap_debug
```

GuardAPI syntax

```
set_ktap_debug parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------|------------|---|
| ktapDebugInterVal | Integer | Required. |
| ktapFunctionNames | String | |
| stapHost | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Say something about the example

```
grdapi set_ktap_debug
```

Related reference

- [S-TAP and inspection engine APIs](#)
-

set_load_balancer_param

This API sets load balancer configuration parameters.

For a list of available parameters and their values, see [Enterprise load balancing configuration parameters](#).

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
set_load_balancer_param parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|---|
| paramName | String | Required. One of the parameters described in Enterprise load balancing configuration parameters . |
| paramType | String | Required. The value must be STAP. |
| paramValue | String | Required. The value for this parameter. |

Related reference

- [Enterprise load balancing configuration parameters](#)
-

set_outliers_detection_demo_mode

This command puts the outlier process in demo mode: time intervals that have no activity at all are ignored and do not affect the statistics.

Attention: Use this mode for demonstrations only. In demo mode, the system is sensitive to small anomalies so that it shows many outliers from relatively normal traffic, including many false positives.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/set_outliers_detection_demo_mode
```

GuardAPI syntax

```
set_outliers_detection_demo_mode
```

This command does not take any parameters. Run it on the system where outlier mining runs.

Examples

To put outliers in demo mode, on the system on which you enter the command:

```
grdapic set_outliers_detection_demo_mode
```

Related concepts

- [Outliers detection](#)

Related reference

- [Outliers detection APIs](#)
-

set_outliers_detection_parameter

Use this command to modify one or more parameters of the outliers detection configuration.

Important: Do not modify the defaults unless you are working with someone knowledgeable in outlier mining.
This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
set_outliers_detection_parameter parameter_name=name parameter_value=value
```

Parameters

| Parameter | Value type | Description |
|--|---------------------------------|--|
| cleanupKeepDays | String | The number of days to retain model data on the collector. Default = 90 |
| sensitiveObjectGroup | Comma separated list of strings | Adds additional object groups (tables, views, and more) to the outliers detection algorithm. Use this command to find a group name: grdap list_group_by_desc desc=<group name> . Factory setting: privUsersGroup=Sensitive Objects |
| sensitiveFileGroup | Comma separated list of strings | Adds additional groups to the outlier detection algorithm. Use this command to find a group name: grdap list_group_by_desc desc=[group name] Factory setting: privUsersGroup=Sensitive Files |
| privUsersGroup | Comma separated list of strings | Adds additional user groups to the outlier detection algorithm. Use this command to find a group name: grdap list_group_by_desc desc=[group name] Factory setting: privUsersGroup=Admin Users |
| minDaysForAlerts | | The number of days of activity required before outlier alerts are produced. The value for this parameter cannot exceed the value of the parameter budgetTrainingDays.
Default = 7 |
| intervalAlertsThreshold | numeric | The score at which an anomaly becomes an outlier. If lowered, the system is more sensitive to anomalies: anomalies with a lower score are issued as outliers and there can be false positives. If raised, then the system is less sensitive to anomalies.
Default = 0.99 |
| maxMessageAlertsTopScores | integer | High volume outliers only. The number of rows in the Details tab of a high volume outlier. The rows present details of the highest scoring anomalies that occurred during the hour.
Default = 500 |
| maxMessageAlertsSampleSizePerAlertType | integer | Non-high-volume outliers only. This is the number of sample anomalies for a summary alert. Non-high-volume outliers have maxMessageAlertsSampleSizePerAlertType sample rows in no specific order since: the score is not relevant for these outliers; no object is newer than another. Default = 500 |
| messageAlertsThreshold | | Internal use only. Do not modify. |
| minNumIntervalsForFirstClustering | integer | The time period, in hours, until users are initially assigned to clusters. Valid values: <ul style="list-style-type: none">• 0: disable clustering, together with clusteringScheduleIntervals=0• 1 and higher: the number of hours until users are clustered
Default = 168 |
| minNumIntervalsForMessageScores | | Internal use only. Do not modify. |
| minNumIntervalsForIntervalScorers | | Internal use only. Do not modify. |
| numOfAnalyzeThreads | | Internal use only. Do not modify. |
| alertsPerDay | integer | The target number of outliers you want to receive per day. The threshold of the alert score is based on statistics for the last budgetTrainingDays parameter. The system sends the outliers with the highest score per hour.
There may be fewer outliers than the value of alertsPerDay in a day simply because there weren't a lot of outliers that day. If there are suddenly many outliers with a score above the threshold, they are reported (and not limited by this parameter). This prevents suppression of an acute situation. |
| budgetTrainingDays | integer | The number of days the system looks back for learning. The value for this parameter cannot be less than the value of the parameter minDaysForAlerts. Default = 14. |
| demoMode | boolean | Used for demo only. Valid values: <ul style="list-style-type: none">• 0: not in demo mode• 1: periods where there's no activity at all are ignored, and do not affect the statistics.
Default = 0 |
| nanny.duration.analysis | | Internal use only. Do not modify. |
| nanny.duration.clean | | Internal use only. Do not modify. |
| nanny.duration.reconfig | | Internal use only. Do not modify. |
| nanny.duration.maintenance | | Internal use only. Do not modify. |
| runCaseAnalysis | boolean | Used for Advanced threat analytics. Valid values: <ul style="list-style-type: none">• false: the case analysis process does not run.• true: the case analysis process runs right after the outlier mining process. |

| Parameter | Value type | Description |
|-----------------------------|------------|---|
| debugMode | boolean | <p>Controls writing debug details into the debug log. Valid values:</p> <ul style="list-style-type: none"> false: debug data is not written into debug tables. true: debug data is written into debug tables. Use this when there is a problem and you want to send “must gather” to Guardium Support. This parameter automatically reverts back to False after 3 days. <ol style="list-style-type: none"> Set the parameter to true. Wait for 3-4 hours. Run ‘data mining’ must gather. Set the parameter back to false. <ul style="list-style-type: none"> Default = false |
| clusteringScheduleIntervals | integer | The frequency at which the clustering algorithm runs. To disable clustering, set both this parameter and minNumIntervalsForFirstClustering = 0 |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> all_managed: execute on all managed units but not the central manager all: execute on all managed units and the central manager group:<group name>: execute on all managed units identified by <group name> host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Add the sensitive object groups 5, 333, and 156 to the outliers detection algorithm:

```
grdapic set_outliers_detection_parameter parameter_name=sensitiveObjectGroupIds parameter_value=5,333,156
```

Related concepts

- [Outliers detection clustering](#)

Related tasks

- [Enabling and disabling outliers detection](#)
- [Grouping users and objects for outlier detection](#)

Related reference

- [Outliers detection APIs](#)

set_outliers_detection_to_factory_settings

This command reverts all outliers parameters to their default, factory settings.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/set_outliers_detection_to_factory_settings
```

GuardAPI syntax

```
set_outliers_detection_to_factory_settings
```

This command does not take any parameters. Run it on the system where outlier mining runs.

Examples

To revert all outliers parameters to their default, factory settings:

```
grdapic set_outliers_detection_to_factory_settings
```

Related concepts

- [Outliers detection](#)

Related reference

- [Outliers detection APIs](#)

set_outliers_user_detection_mode

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/set_outliers_user_detection_mode
```

GuardAPI syntax

```
set_outliers_user_detection_mode parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| mode | String | |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • <code>all_managed</code>: execute on all managed units but not the central manager • <code>all</code>: execute on all managed units and the central manager • <code>group:<group name></code>: execute on all managed units identified by <code><group name></code> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

set_populate_group_from_query_schedule

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/group_query
```

GuardAPI syntax

```
set_populate_group_from_query_schedule parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|--|
| activateSchedule | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true) <p>Default = 1 (true)</p> |
| cronString | String | |
| groupDesc | String | Required. |
| startDate | Date | |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

set_purge_batch_size

This API sets the batch size that is used during purge of data.

When purging a large number of records (10 million or higher), a large batch size setting (500k to 1 million) is the most effective way to purge. Using a smaller batch size or NULL causes the purge to take hours longer. Smaller purges finish quickly, so a large batch size setting is only relevant for large purges. You might need to make a tradeoff in performance and disk space usage. Setting the batch to a larger number increases the speed of the purge but consumes more disk space. Using a low batch size decreases the speed of the purge but does not consume as much disk space.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
set_purge_batch_size parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| batchSize | Long | Required. Number of records. Default = 200000. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To increase the purge batch size from the default (200000) to 300000:

```
grdapi set_purge_batch_size batchSize=300000
```

Related tasks

- [Managing stored data](#)

Related reference

- [Archive, export, import, purge, and restore APIs](#)

set_stap_debug

This command configures the level of detail written to the S-TAP® debug log.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/stap_debug
```

GuardAPI syntax

```
set_stap_debug parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------|------------|---|
| stapDebugInterval | Integer | Required. |
| stapDebugLevel | Integer | Required. Level of debug log.
Unix: Logs are stderr.txt, guard_stap.fam.txt located in the directory specified in tap_log_dir parameter (by default: /tmp/guard_stap). Valid values: <ul style="list-style-type: none">• 0: Disable• 1: Basic debug• 4: Verbose debug• 6: Appserver debug• 10: Exit engine debug. Debug information is logged in both S-TAP log and db2_exit log (db2diag.log).• 11: exit engine debug. Debug information is only logged in db2_exit log (db2diag.log). Windows:Leave at 0 unless directed by IBM® Technical Support. <ul style="list-style-type: none">• 0: Only critical error information. Two start-up debug logs, containing only messages that are related to S-TAP startup, are always generated and saved in bin..\logs. Filename syntax: startup_hostname_timestamp.new and startup_hostname_timestamp.old. Files from bin..\logs get uploaded automatically if upload_feature is on.• 1: All previous messages plus repeatable critical error information. Two "normal" debug logs are saved in bin\StapBuffer. Filename syntax: stap_hostname_timestamp.new and stap_hostname_timestamp.old (from the previous S-TAP session, if it exists). Files from bin\StapBuffer are not uploaded.• 2: Not used.• 3: All messages from level 1, plus brief information about packets sent to a Guardium® system• 4: All messages from level 3, plus local sniffing log.• 5: All messages from level 4, plus network sniffing log.• 6: All messages from level 5, plus heartbeat receiving log.• 7: All messages from level 6, plus miscellaneous debugging information. |
| stapDebugOn | Boolean | Required. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| stapHost | String | Required. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

```
grdapi set_stap_debug stapDebugInterval= stapDebugLevel=1 stapDebugOn=1 stapHost=9.12.56.158
```

set_universal_connector_data_timeout

12.1 and later

This API defined the time duration for which the Universal Connector connection status remains active on the S-TAP Status page if data is not detected.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/setUniversalConnectorDataTimeout
```

GuardAPI syntax

```
set_universal_connector_data_timeout parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|---|
| noDataThresholdInMins | Integer | Number of minutes until the Universal Connector gets disconnected if data is not detected.. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

The following command defines the time duration as 50 minutes after which the Universal Connection gets disconnected.

```
set_universal_connector_data_timeout noDataThresholdInMins=50
```

set_universal_connector_log_level

Run this API to change log level of a running Universal Connector instance (no reload or restart is needed).

This debug level is for the Universal connector, and not the log level of the API itself.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/setUniversalConnectorLogLevel
```

GuardAPI syntax

```
set_universal_connector_log_level parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|--|
| uc_debug_level | String | Required. Valid values: <ul style="list-style-type: none">• <code>all</code>• <code>debug</code>• <code>info</code>• <code>warn</code>• <code>error</code>• <code>fatal</code>• <code>off</code>• <code>trace</code> |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode</p> |

Examples

Set the debug level to warning:

```
grdapi set_universal_connector_log_level uc_debug_level=warn  
Guardium Universal Connector command has been executed.
```

Related concepts

- [Guardium universal connector](#)

Related reference

- [Guardium universal connector APIs](#)

set_user_roles

This API adds or updates the allowed roles for a Guardium user.

Note: Running `set_user_roles` clears all of the current roles for the specified user. Include any existing roles that you want to keep for that user.
This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/user_roles
```

GuardAPI syntax

```
set_user_roles parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| roles | String | Required. The role or roles to assign to this user. To add more than one role, use a comma to separate the roles (but no spaces). |
| userName | String | Required. The name of the user to whom to assign or update roles. |

Example

Set the roles for the user named FredMcDerf (who was created with the [create_user](#) API).

```
grdapi set_user_roles userName="Fred McDerf" roles="admin,dba,diag,cli"
```

Sample output:

```
ID=20001  
Added role (admin).  
Added role (dba).  
Added role (diag).  
Added role (cli).
```

Related concepts

- [User account, password, and authentication CLI Commands](#)

Related reference

- [create_user](#)
- [list_roles](#)

set_ztap_logging_config

This command controls the logging parameters described below.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/ztap_logging_config
```

GuardAPI syntax

```
set_ztap_logging_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| parameter | String | Required. Valid values: <ul style="list-style-type: none">• log_db2z_target: When enabled, targets in db2z protobuf message are logged to GDM_OBJECT in addition to objects from the parser.<ul style="list-style-type: none">◦ 0=off◦ 1=onDefault=0• log_zkey_to_full_sql: When enabled, VSAM or IMS Key values are logged in the full SQL statement for policies using "Log full details."<ul style="list-style-type: none">◦ 0=off◦ 1=onDefault=0• |
| value | String | Required. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To enable logging to GDM_OBJECT:

```
grdapi set_ztap_logging_config parameter=log_db2z_target value=1
```

show_alerter_settings

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/alerter_settings
```

GuardAPI syntax

```
show_alerter_settings parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

show_alerter_smtp_settings

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/alerter_smtp
```

GuardAPI syntax

```
show_alerter_smtp_settings parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

show_alerter_snmp_settings

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/alerter_snmp
```

GuardAPI syntax

```
show_alerter_snmp_settings parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| | | |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

show_alerter_status

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/alerter
```

GuardAPI syntax

```
show_alerter_status parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

show_autodetect_process_status

Use this command to output the auto-discovery process status and the progress summary.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/autodetect_process_status
```

GuardAPI syntax

```
show_autodetect_process_status parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------|------------|--|
| process_name | String | Required. Name of the auto-discovery process |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To see the status and progress of all tasks associated with the auto-discovery process myProcess::

```
grdapi show_autodetect_process_status process_name=myProcess
```

Related concepts

- [Database auto-discovery](#)

Related reference

- [Auto-discovery APIs](#)

show_backup_cm_ip

Run this command on a central manager to list the IP of the backup central manager for each of its managed units.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/show_backup_cm_ip
```

GuardAPI syntax

```
show_backup_cm_ip parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To show the backup central manager IP for this central manager:

```
grdapi show_backup_cm_ip
```

Related concepts

- [Central manager redundancy](#)

Related reference

- [Central management APIs](#)

show_expiring_certificates

12.1 and later This API command shows all the certificates that expire on the system within the specified expiration threshold.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/show_expiring_certificates
```

GuardAPI syntax

```
show_expiring_certificates parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------------|------------|---|
| expirationThreshold | Integer | Required. The value must be greater than or equal to 1. |

Example

The following command shows all the certificates that expire on the system within 40 days.

```
grdapi show_expiring_certificates expirationThreshold=40
```

Sample response:

The following example shows a sample output of an expiring certificate from keystore.

```
[  
{  
  "file_name": "/opt/IBM/Guardium/tomcat/.keystore",  
  "file_type": "KEYSTORE",  
  "certs": [  
    {  
      "expiration_date": "Sun Nov 09 19:00:00 EST 2031",  
      "subject_cn": "DigiCert Global Root CA",  
      "serial_number": XXXXXXXXXXXXXXXXXXXXXXX4346,  
      "alias": "digicertglobalrootca",  
      "fingerprint": "43:48:A0:E9:44:4C:78:CB:26:5E:05:8D:5E:89:44:B4:D8:4F:96:62:BD:26:DB:25:7F:89:34:A4:43:C7:01:61"  
    }  
  ]  
}  
]
```

The following example shows a sample output of an expiring certificate from a PEM file.

```
[  
{  
  "file_name": "/opt/IBM/Guardium/etc/pki/certs/system.cert.pem",  
  "file_type": "PEM",  
  "certs": [  
    {  
      "expiration_date": "Sun Mar 02 19:00:00 EST 2025",  
      "subject_cn": "Guardium",  
      "serial_number": 4,  
      "fingerprint": "CC:D4:B1:A5:FA:DB:E8:69:27:22:E5:23:AB:3B:29:37:B0:90:27:5E:34:1A:60:EF:84:40:CA:BD:21:D7:6D:5C"  
    }  
  ]  
}  
]
```

show_maximum_query_duration

This API displays the current value of the timeout for reports.

You can change the timeout value with `store_maximum_query_duration`.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/show_maximum_query_duration
```

GuardAPI syntax

```
show_maximum_query_duration parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

The following GuardAPI example shows the current timeout value:

```
grdapi show_maximum_query_duration --source-host=localhost --username=admin
```

This command provides the following output:

```
timeout = "200"  
END
```

The following REST API displays the timeout value, which is set to 200 seconds:

```
curl -k --header "Authorization: Bearer deaf8d32-f334-4a9b-976f-163a98afa32a" \  
-i -H "Content-Type:application/json" \  
-X GET https://localhost:8443/restAPI/show_maximum_query_duration
```

This command provides the following JSON output:

```
HTTP/1.1 200 OK  
Cache-Control: private  
Expires: Wed, 31 Dec 1969 19:00:00 EST  
X-FRAME-OPTIONS: SAMEORIGIN  
X-Permitted-Cross-Domain-Policies: none  
X-Content-Type-Options: nosniff  
X-XSS-Protection: 1; mode=block  
...  
Date: Mon, 04 Feb 2019 16:53:20 GMT  
Server: SQL Guard  
{ "timeout": "200" }
```

Related reference

- [kill_running_process](#)
- [list_running_processes](#)
- [store_maximum_query_duration](#)

show_universal_connector_plugins

Run this API to print the Logstash plugin list to output.

This API is relevant for collectors and standalone Guardium systems. The last output to the API is also saved in \$GUARD_VAR/uc/universal-connector-plugins-list.txt.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/showLogstashPlugins
```

GuardAPI syntax

```
show_universal_connector_plugins parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Typical output is:

```
grdapi show_universal_connector_plugins
ID=1
Universal-Connector command has been executed.
Universal-Connector plugins list:
logstash-codec-avro (3.2.3)
logstash-codec-cef (6.0.1)
logstash-codec-collectd (3.0.8)
logstash-codec-dots (3.0.6)
logstash-codec-edn (3.0.6)
logstash-codec-edn_lines (3.0.6)
logstash-codec-es_bulk (3.0.8)
logstash-codec-fluent (3.2.0)
ok
```

Related concepts

- [Guardium universal connector](#)

Related reference

- [Guardium universal connector APIs](#)

solr_repair_analysis

This API is available in Guardium v12.0 and later.

GuardAPI syntax

```
solr_repair_analysis parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------------|------------|---|
| checkDatamartStatus | Boolean | <p>Valid values:</p> <ul style="list-style-type: none">• 0 (false)• 1 (true) <p>Default = 0 (false)</p> |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

start_istap_monitor

This command starts the S-TAP® audit process on IBM i.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/start_istap_monitor
```

GuardAPI syntax

```
start_istap_monitor parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|---|
| datasourceName | String | Required. The name of the Db2 for i datasource. |

Examples

To start the S-TAP audit process on the IBM i server named db21nn:

```
grdapi start_istap_monitor datasourcename=db21nn
```

Related concepts

- [DB2 for IBM i S-TAP](#)

Related reference

- [S-TAP for IBM i APIs](#)

stop_audit_process

Stop an audit process.

You can also stop an audit process from the GUI. Select the **stop_audit_process** command from the Actions menu on the Comply > Tools and Views > Audit Process Log report.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/stop_audit_process
```

GuardAPI syntax

```
stop_audit_process parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| process | Integer | Required. The name of the audit process to stop. |
| run | Integer | Required. The audit process runID. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

stop_autodetect_process

This command stops the run of the tasks associated with the specified process.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/stop_autodetect_process
```

GuardAPI syntax

```
stop_autodetect_process parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| process_name | String | Required. Name of the auto-discovery process |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To stop all tasks associated with the auto-discovery process myProcess:

```
grdapic stop_autodetect_process myProcess
```

Related concepts

- [Database auto-discovery](#)

Related reference

- [Auto-discovery APIs](#)

stop_istap_monitor

This command stops the S-TAP® audit process on IBM i.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/stop_istap_monitor
```

GuardAPI syntax

```
stop_istap_monitor parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|---|
| datasourceName | String | Required. IP or name of the IBM i server. |

Examples

To stop the S-TAP audit process on the IBM i server named db21nn:

```
grdapic start_istap_monitor datasourceName=db21nn
```

Related concepts

- [DB2 for IBM i S-TAP](#)

Related reference

- [S-TAP for IBM i APIs](#)

stop_restart_alerter

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/alerter
```

GuardAPI syntax

```
stop_restart_alerter parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| action | String | Required. Valid values: <ul style="list-style-type: none"><code>stop</code><code>restart</code> |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"><code>all_managed</code>: execute on all managed units but not the central manager<code>all</code>: execute on all managed units and the central manager<code>group:<group name></code>: execute on all managed units identified by <code><group name></code>host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

stop_solr

This command stops the solr process on the specified Guardium® system(s).

This command can be run on all types of Guardium systems.

This API is available in Guardium V10.6 and later.

GuardAPI syntax

```
stop_solr parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| stop_all | Boolean | <p>Valid values:</p> <ul style="list-style-type: none">• 0 (false)• 1 (true) <p>Default = 0 (false)</p> |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapi stop_solr stop_all=true
```

Related reference

- [Solr APIs](#)

stop_universal_connector

Run this command to stop the Guardium universal connector on the local or the specified collectors.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/stopUniversalConnector
```

GuardAPI syntax

```
stop_universal_connector parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To stop the Guardium universal connector on your local system:

```
grdap> stop_universal_connector  
ID=0  
Universal-Connector was disabled.  
ok
```

Related concepts

- [Guardium universal connector](#)

Related reference

- [Guardium universal connector APIs](#)

store_maximum_query_duration

Use this API to change the timeout value for queries and reports.

Use store_maximum_query_duration in cases where you have very large or long-running reports to increase the length of time before the report times out. You can also set this value from the Running Status Monitor pane on the administrator portal.

Note: If you set this value greater than the default, you can overload the system with query processing.

If a report (or query) continues to run past the designated timeout period, you can stop the report by using the [kill_running_process](#) API.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/store_maximum_query_duration
```

GuardAPI syntax

```
store_maximum_query_duration parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| durationSeconds | Integer | Required. Default = 180 (seconds). |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

The following GuardAPI example sets the timeout value to 200 seconds.

```
>grdap> store_maximum_query_duration durationSeconds="200"  
ID=0
```

This command provides the following output:

```
"Query Timeout SuccessFully Updated"  
ok
```

The following REST API sets the timeout value to 200 seconds:

```
curl -k --header "Authorization:Beaf8d32-f334-4a9b-976f-163a98afa32a" -i -H "Content-Type:application/json"  
-X PUT -d '{"durationSeconds":"200"}' https://localhost:8443/restAPI/store_maximum_query_duration
```

This command provides the following JSON output:

```
HTTP/1.1 200 OK  
Cache-Control: private  
Expires: Wed, 31 Dec 1969 19:00:00 EST  
X-FRAME-OPTIONS: SAMEORIGIN  
X-Permitted-Cross-Domain-Policies: none  
X-Content-Type-Options: nosniff
```

```
X-XSS-Protection: 1; mode=block
.
.
Date: Mon, 04 Feb 2019 17:08:54 GMT
Server: SQL Guard
{ "ID": 0, "Message": "Query Timeout SuccessFully Updated" }
```

Related concepts

- [Running Query Monitor](#)

Related reference

- [kill_running_process](#)
- [list_running_processes](#)
- [show_maximum_query_duration](#)

store_sql_credentials

This command defines the credentials of the connection between an S-TAP® and an Oracle server that is used for Oracle Unified Auditing.

Note: The password can also be defined in the S-TAP Control page, with Send Command.
This API is available in Guardium V11.1 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/stap
```

GuardAPI syntax

```
store_sql_credentials parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| password | String | Required. Password for logging in to the Oracle DB. |
| stapHost | String | Required. The hostname of the S-TAP that connects to this Oracle DB instance. For valid values, call store_sql_credentials from the command line with --help=true . |
| username | String | Required. User name for logging in to the Oracle DB. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

store_stap_approval

This command controls the S-TAP® certification feature; when enabled only approved S-TAPs can access the Guardium® system.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/stap_approval
```

GuardAPI syntax

```
store_stap_approval parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| isNeeded | Boolean | Required. Valid values: <ul style="list-style-type: none">• 0: feature is disabled• 1: feature is enabled |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To enable S-TAP certification on the system on which you enter the command:

```
grdapic store_stap_approval
```

Related concepts

- [Inspection engine configuration](#)

Related tasks

- [Allow \(approve\) S-TAP connection to Guardium \(S-TAP Certification\)](#)
- [Linux-UNIX: Configuring an inspection engine](#)
- [Windows: Configuring an inspection engine](#)

Related reference

- [S-TAP and inspection engine APIs](#)

switch_outliers_user_mode

This API is available in Guardium V11.2 and later.

GuardAPI syntax

```
switch_outliers_user_mode parameter=value
```

Parameters

test_datasource_connection

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/test_connection
```

GuardAPI syntax

```
test_datasource_connection parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| name | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

test_hashicorp_connection

Use this command to test the connection for a HashiCorp configuration.

This API is available in Guardium® v11.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/test_hashicorp_connection
```

GuardAPI syntax

```
test_hashicorp_connection parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| name | String | The name of the HashiCorp configuration. |

Example

```
grdapi test_hashicorp_connection name="No SSL User and password API"
ID=1
Test Connection was successful for hashicorp config.
ok
```

Related concepts

- [Datasource credential management APIs](#)

test_solr

This command runs diagnostics on the solr internal database on your system. The output indicates if there are any problems, and gives detailed instructions on resolving them.

This API is available in Guardium V11.0 and later.

GuardAPI syntax

```
test_solr parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| details | Boolean | <p>Can be used on managed units, central managers, and stand-alone systems. On managed units run with details=true only. On the central manager, both options are valid. Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true) <p>Default = 0 (false)</p> |

| Parameter | Value type | Description |
|-----------------|------------|---|
| logToFile | Boolean | <p>Outputs results to file. Can be used on managed units, central managers, and stand-alone systems. Log file location: /var/IBM/Guardium/log/solr_test.json. Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true) <p>Default = 1 (true)</p> |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapi test_solr
```

Sample response:

```
Look at the following file for results; if the target host was specified, look on the target host
machine:/var/IBM/Guardium/log/solr_test.json
ok
```

Related reference

- [Solr APIs](#)

Related information

- [Troubleshooting the investigation dashboard and enterprise search](#)

test_solr_cluster_status

This API is available in Guardium v12.0 and later.

GuardAPI syntax

```
test_solr_cluster_status parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

test_solr_connectivity

This command checks bi-directional communication between the central manager and its managed units on port 8983; and it checks communication from the managed units to the central manager on port 9983 (this port is open only on the central manager).

This API is available in Guardium V11.0 and later.

GuardAPI syntax

```
test_solr_connectivity parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| logToFile | Boolean | Outputs results to file. Log file location: /var/IBM/Guardium/log/solr_connection_test.json. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

```
grdapi test_solr_connectivity
```

Sample response:

```
Look at the following file for results; if the target host was specified, look on the target host
machine:/var/IBM/Guardium/log/solr_connection_test.json
ok
```

Related reference

- [Solr APIs](#)

test_solr_hardware_requirements

This command checks if the system hardware meets the Solr hardware requirements.

This API is available in Guardium V11.0 and later.

GuardAPI syntax

```
test_solr_hardware_requirements parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| logToFile | Boolean | Outputs results to file. Log file location: /var/IBM/Guardium/log/solr_test_hardware_requirements.json. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

```
grdapi test_solr_hardware_requirements logToFile=1
```

Sample response:

```
Look at the following file for results; if the target host was specified, look on the target host  
machine:/var/IBM/Guardium/log/solr_test_hardware_requirements.json  
ok
```

Related reference

- [Solr APIs](#)

Related information

- [Troubleshooting the investigation dashboard and enterprise search](#)

unassign_load_balancer_groups

This API removes the assignment of a managed unit group from an application or S-TAP® group.

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
unassign_load_balancer_groups parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------|------------|--|
| appGroupName | String | Required. The application or S-TAP group name. |
| muGroupName | String | Required. The managed unit group name. |

Related reference

- [assign_load_balancer_groups](#)

unassign_qr_condition_from_action

This command removes the specified query condition from the specified action.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/qr_condition_to_action
```

GuardAPI syntax

```
unassign_qr_condition_from_action parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|---|
| actionName | String | Required. The unique name of the query rewrite action. |
| conditionName | String | Required. The condition that is getting removed from the action. |
| definitionName | String | Required. The query rewrite definition that is associated with this action. |

Examples

```
grdapi unassign_qr_condition_to_action definitionName="case 15" actionName="qr action15_2" conditionName="qr cond15_2"
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

uninstall_policy_rule

This command uninstalls one or more rules from a specified policy.

Specify multiple rules by using a pipe (|) character as a delimiter between rule names.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/uninstall_policy_rule
```

GuardAPI syntax

```
uninstall_policy_rule parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| policy | String | Required. The name of the policy. |
| ruleName | String | Required. The name of the rule or rules to uninstall. Use a pipe () character as a delimiter between rule names. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI examples

Uninstall a single policy rule:

```
grdapiclnt uninstall_policy_rule policy="Hadoop Policy" ruleName="Low interest Objects: Allow"
```

Uninstall multiple policy rules:

```
grdapiclnt uninstall_policy_rule policy="Hadoop Policy" ruleName="Low interest Objects: Allow|Low Interest Commands: Allow"
```

universal_connector_cleanup

This API is available in Guardium v11.4 and later.

The API uninstalls all the Universal Connector connections in the Managed Unit, and cleans the relevant data. By using this api UC is in freshly installed state.

REST API syntax

This API is available as a REST service with the **POST** method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/ucCleanUp
```

GuardAPI syntax

```
universal_connector_cleanup parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

universal_connector_disable_metrics

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/updateMetricsSetting
```

GuardAPI syntax

```
universal_connector_disable_metrics parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| enable_metrics | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true) <p>Default = 0 (false)</p> |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

universal_connector_enable_metrics

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/updateMetricsSetting
```

GuardAPI syntax

```
universal_connector_enable_metrics parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| | | |

| Parameter | Value type | Description |
|-----------------|------------|---|
| enable_metrics | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true) <p>Default = 1 (true)</p> |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

universal_connector_keystore_add

This API is available in Guardium v11.4 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/universalConnectorKeystore
```

GuardAPI syntax

```
universal_connector_keystore_add parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| key | String | Required. |
| override | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true) <p>Default = 0 (false)</p> |
| password | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

universal_connector_keystore_list

This API is available in Guardium v11.4 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/universalConnectorKeystore
```

GuardAPI syntax

```
universal_connector_keystore_list parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

universal_connector_keystore_remove

This API is available in Guardium v11.4 and later.

REST API syntax

This API is available as a REST service with the **DELETE** method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/universalConnectorKeystore
```

GuardAPI syntax

```
universal_connector_keystore_remove parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| key | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

universal_connector_troubleshooting

This API is available in Guardium v11.5 and later.

REST API syntax

This API is available as a REST service with the **GET** method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/troubleshooting
```

GuardAPI syntax

```
universal_connector_troubleshooting parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

universal_connector_update_proxy

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/ucUpdateProxy
```

GuardAPI syntax

```
universal_connector_update_proxy parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| httpProxyIP | String | Required. |
| httpProxyPort | String | Required. |
| httpsProxyIP | String | Required. |
| httpsProxyPort | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

unregister_unit

REST API syntax

12.1 and later This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/unregister_unit
```

GuardAPI syntax

```
unregister_unit parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|-------------|
| unitIpList | String | Required. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

unschedule_datamart

This command stops extraction of the specified datamart.

This API is available in Guardium V10.5 and later.

REST API syntax

This API is available as a REST service with the `DELETE` method. Call this API as follows:

```
DELETE https://[Guardium hostname or IP address]:8443/restAPI/datamartSchedule
```

GuardAPI syntax

```
unschedule_datamart parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| datamart_name | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To unschedule the data mart Export:Full SQL

```
unschedule_datamart datamart_name="Export:Full SQL"
```

Related concepts

- [Data mart](#)

Related reference

- [Data mart APIs](#)

update_alias

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/alias
```

GuardAPI syntax

```
update_alias parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------|------------|---|
| dbValue | String | Required. |
| groupTypeDesc | String | Required. For valid values, call update_alias from the command line with --help=true. |
| newAliasValue | String | Required. |
| oldAliasValue | String | Required. |

update_assessment

This command updates a security assessment.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/assessment
```

GuardAPI syntax

```
update_assessment parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|--|
| assessmentDescription | String | Required. The value for this parameter must match an existing record in a security assessment. |
| newDescription | String | |
| processName | String | |

Example

```
grdapi update_assessment assessmentDescription=Assess1 filterClientIP=192.168.1.1.
```

update_assessment_test

This command updates a test in a security assessment.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/assessment_test
```

GuardAPI syntax

```
update_assessment_test parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|---|
| assessmentDescription | String | Required. |
| datasourceType | String | For valid values, call update_assessment_test from the command line with --help=true. |
| exceptionsGroup | String | |
| explanation | String | |
| ExternalReference | String | |
| fromDate | String | |

| Parameter | Value type | Description |
|-----------------|------------|--|
| severity | String | Valid values: <ul style="list-style-type: none">• <i>Critical</i>• <i>Major</i>• <i>Minor</i>• <i>Caution</i>• <i>Info</i> |
| testDescription | String | Required. |
| threshold | String | |
| toDate | String | |

update_aws_secrets_manager_config

Use this command to edit an AWS secrets configuration.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/aws_secrets_manager
```

GuardAPI syntax

```
update_aws_secrets_manager_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------------|------------|---|
| access_key_id | String | |
| auth_type | String | Required. Valid values: <ul style="list-style-type: none">• <i>Security-Credentials</i>• <i>IAM-Role</i>• <i>IAM-Instance-Profile</i> |
| name | String | Required. For valid values, call update_aws_secrets_manager_config from the command line with <code>--help=true</code> . |
| role_arn | String | The Role Amazon Resource Name (ARN) |
| secret_access_key | String | |
| secret_key_password | String | The Secret key label for the password |
| secret_key_username | String | The Secret key label for the username |

Examples

```
grdapic update_aws_secrets_manager_config name="GRDAPI Security-Credentials"
access_key_id="home_markdown_jenkins_workspace_Transform_in_SSMPHH_12.x_com.ibm.guardium.doc.reference_grdapic_update_aws_secrets_manager_config_AABBCC123" secret_access_key="XXYYZZ321" secret_key_password="password" secret_key_username="username"

grdapic update_aws_secrets_manager_config name="GRDAPI IAM-Role" auth_type="IAM-Role"
role_arn="arn:aws:iam::123456789:role/AWS_Secret_ManagerReadWrite_role"
access_key_id="home_markdown_jenkins_workspace_Transform_in_SSMPHH_12.x_com.ibm.guardium.doc.reference_grdapic_update_aws_secrets_manager_config_aabbcc123" secret_access_key="abcdefg" secret_key_password="password" secret_key_username="username"

grdapic update_aws_secrets_manager_config name="GRDAPI IAM-Instance-Profile2" auth_type="IAM-Instance-Profile2"
secret_key_password="password" secret_key_username="username"
```

update_cas_host_instance

This command enables or disables a Configuration Auditing System (CAS) template.

Use this command to enable or disable a CAS host instance by setting the enabled parameter to 1 (enabled) or 0 (disabled). Use the [list_cas_host_instances](#) API to find the dataSourceName and templateSetLabel parameter values.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/cas_host_instance
```

GuardAPI syntax

```
update_cas_host_instance parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|---|
| datasourceName | String | Required. The data source used for this host instance. |
| enabled | Boolean | Required. Enables or disables the host instance. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| templateSetLabel | String | Required. The name of the template set that is associated with the host instance. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

The following example shows how to find and update information within a CAS host instance:

1. Call `list_cas_host_instances` to find the `datasourceName` and `templateSetLabel`.

```
grdapi list_cas_host_instances hostName=9.70.150.111
Id, datasourceName(#), datasourceName, templateSetLabel(#), templateSetLabel, hostName, osType, dbType
c0d2327c8dd550549f2579ab44819a54c3db5e6a, 20002, System (9.70.150.111), 16, Default Unix Template Set, 9.70.150.129, UNX, N_A
ok
```

2. Call `update_cas_host_instance`, and enable the host instance

```
grdapi update_cas_host_instance datasourceName=20002 templateSetLabel=16 enabled=1
ID=c0d2327c8dd550549f2579ab44819a54c3db5e6a
ok
```

update_cas_template

This command modifies specified parameters in a Configuration Auditing System (CAS) template.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/cas_template
```

GuardAPI syntax

```
update_cas_template parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| enabled | Boolean | Enable or disable the template. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |

| Parameter | Value type | Description |
|-----------------|------------|---|
| isEditable | Boolean | Set the ability for users to modify to the template. Valid values: <ul style="list-style-type: none"> • 0 (false) • 1 (true) |
| period | Integer | Change the number of minutes to wait between tests. |
| saveData | Boolean | Enable or disable whether to save previous versions of the template item. Valid values: <ul style="list-style-type: none"> • 0 (false) • 1 (true) |
| template | String | A new name for this template. |
| templateId | Long | Required. The internal ID for this template. If needed you can find the template ID by using the list_cas_templates API. |
| useMD5 | Boolean | Enables or disable using the uses the MD5 algorithm. Valid values: <ul style="list-style-type: none"> • 0 (false) • 1 (true) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

The following example shows how to find and update information within a CAS template:

1. Call `list_cas_templates` to find the template ID and other information about a template to update.

```
grdapi list_cas_templates templatesetLabel=testSet
ID=20001
Id, auditType, template, enabled, period, useMD5, saveData, isEditable
20000, FILE, tempTest, true, 3600, false, false, true
ok
```

2. Call `update_cas_template` to change the name and time period.

```
grdapi update_cas_template templateId=20000 template=newName period=5
ID=20000
ok
```

3. Call `list_cas_templates` again to show the changes/

```
grdapi list_cas_templates templatesetLabel=testSet
ID=20001
Id, auditType, template, enabled, period, useMD5, saveData, isEditable
20000, FILE, newName, true, 5, false, false, true
ok
```

update_classifier_action

This command updates classifier actions.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/classifier_action
```

GuardAPI syntax

```
update_classifier_action parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------------|------------|--|
| accessPolicy | String | |
| accessRuleAction | String | |
| actionName | String | Required. |
| actionType | String | Required. |
| actualMemberContent | String | |
| commandsGroup | String | |
| description | String | |
| excludeObjectGroup | String | |
| includeField | Boolean | Valid values:
<ul style="list-style-type: none"> • 0 (false) • 1 (true) Default = 0 (false) |
| includeServerIP | Boolean | Valid values:
<ul style="list-style-type: none"> • 0 (false) • 1 (true) Default = 0 (false) |
| notificationType | String | |
| objectFieldGroup | String | |
| objectGroup | String | |
| policyName | String | Required. |
| privacySet | String | |
| receiver | String | |
| replaceGroupContent | Boolean | Valid values:
<ul style="list-style-type: none"> • 0 (false) • 1 (true) Default = 0 (false) |
| ruleDescription | String | |
| ruleName | String | Required. |
| SchemaGroup | String | |
| severity | String | |

update_classifier_document_rule

This API is available in Guardium v11.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/classifier_document_rule
```

GuardAPI syntax

```
update_classifier_document_rule parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------------------|------------|---|
| calculateConfidenceScore | Boolean | Valid values:
<ul style="list-style-type: none"> • 0 (false) • 1 (true) Default = 1 (true) |
| category | String | For valid values, call update_classifier_document_rule from the command line with <code>--help=true</code> . |
| classification | String | |
| collectionNameLike | String | |
| collectionTypeCollection | Boolean | Valid values:
<ul style="list-style-type: none"> • 0 (false) • 1 (true) Default = 1 (true) |

| Parameter | Value type | Description |
|--------------------------------|------------|---|
| collectionTypeView | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| compareToValuesInGroup | String | |
| compareToValuesInSQL | String | |
| continueOnMatch | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| continueWithUnmatchedFieldOnly | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| dataTypes | String | |
| description | String | |
| evaluationName | String | |
| excludeCollection | String | |
| excludeCollectionField | String | |
| excludeDatabaseName | String | |
| fieldNameLike | String | |
| fireOnlyWithMarker | String | |
| hitPercentage | Integer | |
| policyName | String | Required. |
| ruleName | String | Required. |
| ruleType | String | Required. |
| searchExpression | String | |
| searchLike | String | |
| showUniqueValues | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| skipEmptyNull | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| uniqueValueMask | String | |

update_classifier_log_level

This command updates the classifier log level.

This API is available in Guardium V10.6 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/classifier_log_level
```

GuardAPI syntax

```
update_classifier_log_level parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|---|
| logLevel | String | <p>Required.
Valid values:</p> <ul style="list-style-type: none"> • DEBUG • ERROR • FATAL • INFO • WARN • TRACE <p>The DEBUG value logs details about the classification scan. For example, metadata from the scanned database such as table and column names is logged, but actual data from the database is not logged.</p> <p>Important: Restart the job queue using the <code>restart_job_queue_listener</code> API after changing the log level.</p> |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

```
grdapi update_classifier_log_level logLevel=INFO
```

update_classifier_policy

This command updates classification policies.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/classifier_policy
```

GuardAPI syntax

```
update_classifier_policy parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|--|
| category | String | Required. For valid values, call <code>update_classifier_policy</code> from the command line with <code>--help=true</code> . |
| classification | String | Required. |
| description | String | |
| newName | String | |
| policyName | String | Required. |

Examples

```
grdapi update_classifier_policy policyName=access_policy classification=class_01 category=Access
```

update_classifier_process

This command updates classification processes.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/classifier_process
```

GuardAPI syntax

```
update_classifier_process parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|--|
| comprehensive | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| datasourceGroups | String | |
| datasourceNames | String | |
| datasourceType | String | Valid values: <ul style="list-style-type: none">• DOCUMENT• RELATIONAL Default = RELATIONAL |
| includeInternalTables | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false)

Enabling includeInternalTables indicates that you want to scan internal system databases and schema used by the database software provider. Internal system databases and schema are unlikely to contain sensitive data and are not scanned by default. When including internal tables, verify that the classifier datasource user has sufficient privileges to scan the internal databases and schema. Insufficient privileges may result in unexpected classification policy errors.

To view and edit the databases and schema impacted by the includeInternalTables parameter, use the Group Builder to edit one of the predefined Excluded Classification groups. |
| newName | String | |
| policyName | String | |
| processName | String | Required. |
| sampleSize | Integer | |

Examples

```
grdapi update_classifier_process datasourceNames=datasource_01,datasource_02 policyName=access_policy  
processName=APITEST_Clps_10001_1 comprehensive=0 sampleSize=3000
```

update_classifier_rule

This command updates classification rules.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/classifier_rule
```

GuardAPI syntax

```
update_classifier_rule parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------------------|------------|--|
| calculateConfidenceScore | Boolean | Calculate a confidence score. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| category | String | Required. For valid values, call <code>create_classifier_rule</code> from the command line with <code>--help=true</code> . |
| classification | String | Required. |

| Parameter | Value type | Description |
|----------------------------------|------------|---|
| columnNameLike | String | |
| compareToValuesInGroup | String | |
| compareToValuesInSQL | String | |
| continueOnMatch | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| continueWithUnmatchedColumnsOnly | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| dataTypes | String | |
| description | String | |
| evaluationName | String | |
| excludeSchemaName | String | |
| excludeTable | String | |
| exclude TableColumn | String | |
| fireOnlyWithMarker | String | |
| hitPercentage | Integer | |
| maxLength | Integer | |
| minLength | Integer | |
| policyName | String | Required. |
| ruleName | String | Required. |
| ruleType | String | Required. |
| searchExpression | String | |
| searchLike | String | |
| showUniqueValues | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true)
Default = 0 (false) |
| skipEmptyNull | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true)
Default = 0 (false) |
| tableNameLike | String | |
| tableTypeSynonym | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true)
Default = 0 (false) |
| tableTypeSystemTable | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true)
Default = 0 (false) |
| tableTypeTable | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true)
Default = 1 (true) |
| tableTypeView | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true)
Default = 0 (false) |
| uniqueValueMask | String | |

update_cloud_datasource

Updates the cloud datasource configuration (cloud database service protection).

This API is available in Guardium V10.1 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/cloud_datasource
```

GuardAPI syntax

```
update_cloud_datasource parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------------|------------|--|
| cloudTitle | String | Required. Name of cloud account already defined in Guardium. Required. For valid values, call update_cloud_datasource from the command line with --help=true .
For more information, see create_cloudTitle . |
| conProperty | String | Use only if additional connection properties must be included on the JDBC URL to establish a JDBC connection with this datasource. The required format is property=value, where each property and value pair is separated from the next by a comma. |
| customURL | String | Connection string to the datasource; otherwise connection is made using host, port, instance, properties, etc. of the previously entered fields. This is useful, for example, when creating Oracle Internet Directory (OID) connections. |
| cyberarkConfigName | String | The name of the CyberArk configuration on your Guardium system. For valid values, call update_cloud_datasource from the command line with --help=true . |
| cyberarkObjectName | String | The CyberArk object name for the Guardium datasource. |
| dbInstanceAccount | String | Database Account Login Name that is used by CAS. |
| dbInstanceDirectory | String | Directory where database software was installed that is used by CAS. |
| dbName | String | For a Db2® or Oracle datasource, enter the schema name. For others, enter the database name. |
| description | String | A longer description of the datasource. |
| externalPasswordType | String | For valid values, call update_cloud_datasource from the command line with --help=true . |
| host | String | Required. The host name or the IP address of the server hosting the DB you are monitoring. |
| importServerSSLcert | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| KerberosConfigName | String | Name of Kerberos configuration already defined in Guardium system. |
| name | String | Required. A unique name for the datasource in the Guardium system. |
| new name | string | Specifies a new name for the datasource. |
| objectLimit | Integer | Required. The maximum number of sensitive objects found in the classification process that are added automatically to the list of audited objects. Default = 20. |
| password | String | Password for user. |
| port | Integer | Port number. |
| primaryCollector | Integer | The collector that extracts the audit data from the cloud database. |
| region | String | Required for AWS only. For valid values, call update_cloud_datasource from the command line with --help=true . |
| savePassword | Boolean | Saves and encrypts your authentication credentials on the Guardium appliance. Required if you are defining a datasource with an application that runs as a scheduled task (as opposed to on-demand). When set to yes, login name and password are required. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true)
Default = 1 (true) |
| serviceName | String | Required for Oracle, Informix®, Db2, and IBM® i. For a Db2 datasource enter the database name, for others enter the service name. |
| severity | String | Severity Classification (or impact level) for the datasource. For valid values, call update_cloud_datasource from the command line with --help=true . |
| shared | String | Set to true or Shared to share with other applications. To share the datasource with other users, you need to assign roles from the GUI. Valid values: <ul style="list-style-type: none">• Shared• Not Shared• true• false |
| useExternalPassword | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| useKerberos | Boolean | Set to 1 (true) to use Kerberos authentication. If true, KerberosConfigName is required. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |

| Parameter | Value type | Description |
|-----------------|------------|---|
| useLDAP | Boolean | Set to 1 (true) to use LDAP. Valid values: <ul style="list-style-type: none"> • 0 (false) • 1 (true) |
| user | String | User for the datasource. If used, password must also be specified. |
| useSSL | Boolean | Set to 1 (true) to use SSL authentication. Valid values: <ul style="list-style-type: none"> • 0 (false) • 1 (true) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

Say something about the example

```
grdapi update_cloud_datasource
```

update_computed_attribute

This API updates an existing custom attribute that is calculated based on a specified expression.

To help prevent an SQL injection attack, the following words and characters are not allowed in computed attributes:

ALTER, CREATE, DELETE, DROP, INSERT, TRUNCATE, UPDATE, semicolon (;), double-dash (--), or slash-asterisk /*)

For more information, see [create_computed_attribute](#).

This API is available in Guardium V9.5 and later.

The REST API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/computed_attribute
```

GuardAPI syntax

```
update_computed_attribute parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|---|
| attributeLabel | String | Required. The name of the computed attribute to update. |
| entityLabel | String | Required. The name of the main entity with which the attribute is associated. |
| newexpression | String | Required. The updated expression for this attribute. |
| oldexpression | String | Required. The original expression for this attribute. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Related reference

- [create_computed_attribute](#)

update_constant_attribute

This API is available in Guardium V9.5 and later.

The REST API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/constant_attribute
```

GuardAPI syntax

```
update_constant_attribute parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| attributeLabel | String | Required. |
| entityLabel | String | Required. |
| newConstant | String | Required. |
| oldConstant | String | Required. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

update_custom_table_ldap_import

This command updates the configuration of a custom table to import data from LDAP.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/custom_data_ldap
```

GuardAPI syntax

```
update_custom_table_ldap_import parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------------------------|---|
| activateSchedule | Boolean-Constant values list | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| attributeMapping | String | |
| baseDN | String | |
| clearTable | Boolean-Constant values list | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| cronString | String | |
| filter | String | |
| filterScope | String | Valid values: <ul style="list-style-type: none">• <i>one-level</i>• <i>sub-tree</i> |
| hostName | String | |
| importId | Integer | Required. |
| importLimit | Integer | |
| password | String | |
| port | Integer | |
| serverType | String | Valid values: <ul style="list-style-type: none">• <i>Active Directory</i>• <i>Novell Directory</i>• <i>Open LDAP</i>• <i>Sun ONE Directory</i>• <i>z/OS Security Server</i>• <i>Tivoli Directory</i> |
| startDate | Date | |
| userName | String | |
| useSSL | Boolean-Constant values list | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • <i>all_managed</i>: execute on all managed units but not the central manager • <i>all</i>: execute on all managed units and the central manager • <i>group:<group name></i>: execute on all managed units identified by <i><group name></i> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <i>api_target_host=10.0.1.123</i>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <i>api_target_host=10.0.1.123</i>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

update_cyberark_config

This command updates the CyberArk configuration on your Guardium system. Obtain the application IDs, corresponding safe names, and folder names from your CyberArk administrator.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/cyberark
```

GuardAPI syntax

```
update_cyberark_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| applicationId | String | This is a unique variable that is created on CyberArk. |
| folderName | String | The name of the folder where the CyberArk safe is located. |
| name | String | Required. The name that is used to configure the Guardium datasource to access the CyberArk vault. |
| safeName | String | The name of the CyberArk safe that is assigned to the applicationId. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

update_datamart

This command updates the start time or adds a comment to a user-defined or predefined data mart export.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/update_datamart
```

GuardAPI syntax

```
update_datamart parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------------------|----------------|--|
| Comment | String | Comment about the change you make. |
| initial_start | Date | Valid values: <ul style="list-style-type: none">• <>: current time• YYYY-MM-DD hh:mm:ss |
| extracted_date_max_limit | java.util.Date | |
| linesPerFile | Integer | |
| Name | String | Required. Data mart name. |

Examples

To set the start time of data mart Export:Full SQL to midnight on 1 September 2019:

```
update_datamart name="Export:Full SQL" initial_start 2019-09-01 00:00:00
```

Related concepts

- [Data mart](#)

Related reference

- [Data mart APIs](#)

update_datamart_copy_file_threadpool_params

This API is available in Guardium v11.4 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/update_datamart_copy_file_threadpool_params
```

GuardAPI syntax

```
update_datamart_copy_file_threadpool_params parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------------|------------|---|
| corePoolSize | Integer | |
| keepAliveSec | Integer | |
| maxPoolSize | Integer | |
| maxTasksWaitin
gSize | Integer | |
| shouldRestart | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

update_datasource_by_id

This command updates a datasource definition identified by an identification key.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/update_datasource_by_id
```

GuardAPI syntax

```
update_datasource_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------------|------------|---|
| awsSecretsManagerConfigName | String | For valid values, call update_datasource_by_id from the command line with <code>--help=true</code> . |
| conProperty | String | Use only if additional connection properties must be included on the JDBC URL to establish a JDBC connection with the datasource. Note: For a Sybase database with a default character set of Roman8, enter the following property: <code>CHARSET=utf8</code> . |
| customProps | String | |
| customURL | String | Defines the connection string to the datasource. By default, the connection is made using the host, port, instance, and other properties defined by the API parameters. This is useful, for example, when creating Oracle Internet Directory (OID) connections. |
| cyberarkConfigName | String | The name of the CyberArk configuration on your Guardium system. For valid values, call update_datasource_by_id from the command line with <code>--help=true</code> . |
| cyberarkObjectName | String | The CyberArk object name for the Guardium datasource. |
| dbInstanceAccount | String | The database account login name to be used by CAS. |
| dbInstanceDirectory | String | The database installation directory to be used by CAS. |

| Parameter | Value type | Description |
|-------------------------|------------|---|
| dbName | String | For a DB2® datasource, the database name. |
| description | String | A description of the datasource. |
| externalPassword | String | For valid values, call update_datasource_by_id from the command line with --help=true. |
| hashicorpChildNameSpace | String | |
| hashicorpConfigName | String | |
| hashicorpPath | String | |
| hashicorpRole | String | |
| host | String | The host name or the IP address of the datasource. |
| id | Integer | Required. The identification key of the datasource to be updated. |
| importServerSSLcert | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| KerberosConfigName | String | |
| newName | String | Defines a new name for the datasource. The new name must be unique for a datasource on the system.x |
| password | String | The password for the account identified by the user parameter. If defined, the user parameter must also be used. |
| port | Integer | The port number of the datasource. |
| region | String | For AWS only. For valid values, call update_datasource_by_id from the command line with --help=true. |
| savePassword | Boolean | If enabled, savePassword saves and encrypts authentication credentials on the Guardium system. This is required when defining a datasource with an application that runs as a scheduled task (as opposed to on demand). When set to 1, the user and password parameters are required.
Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| secretName | String | |
| serviceName | String | For an Oracle datasource, the service name. |
| severity | String | Severity classification (or impact level) for the datasource.
For valid values, call update_datasource_by_id from the command line with --help=true. |
| shared | String | If set to true, share the datasource with other applications. To share the datasource with other users, assign roles from the GUI.
Valid values: <ul style="list-style-type: none">• Shared• Not Shared• true• false |
| useExternalPassword | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| useKerberos | Boolean | If set to 1, use Kerberos authentication. When set to 1, the KerberosConfigName is required.
Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| useLDAP | Boolean | If set to 1, use LDAP.
Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| user | String | The user name for the datasource. If defined, the password parameter must also be used. |
| useSSL | Boolean | If set to 1, use SSL authentication.
Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| walletZip | String | |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

Use this command to change the name of the database with identification key 2 to chicken DB2:

```
grdapi update_datasource_by_id id=2 newName="chicken DB2"
```

update_datasource_by_name

This command updates a datasource definition identified by name.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/update_datasource_by_name
```

GuardAPI syntax

```
update_datasource_by_name parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------------|------------|---|
| awsSecretsManagerConfigName | String | For valid values, call <code>update_datasource_by_name</code> from the command line with <code>--help=true</code> . |
| conProperty | String | Use only if additional connection properties must be included on the JDBC URL to establish a JDBC connection with the datasource. Note: For a Sybase database with a default character set of Roman8, enter the following property: <code>CHARSET=utf8</code> . |
| customProps | String | |
| customURL | String | Defines the connection string to the datasource. By default, the connection is made using the host, port, instance, and other properties defined by the API parameters. This is useful, for example, when creating Oracle Internet Directory (OID) connections. |
| cyberarkConfigName | String | The name of the CyberArk configuration on your Guardium system. For valid values, call <code>update_datasource_by_name</code> from the command line with <code>--help=true</code> . |
| cyberarkObjectName | String | The CyberArk object name for the Guardium datasource. |
| dbInstanceAccount | String | The database account login name to be used by CAS. |
| dbInstanceDirectory | String | The database installation directory to be used by CAS. |
| dbName | String | For a DB2® datasource, the database name. |
| description | String | A description of the datasource. |
| externalPasswordType | String | For valid values, call <code>update_datasource_by_name</code> from the command line with <code>--help=true</code> . |
| hashicorpChildNamespace | String | |
| hashicorpConfigName | String | |
| hashicorpPath | String | |
| hashicorpRole | String | |
| host | String | The host name or the IP address of the datasource. |
| importServerSSLcert | Boolean | Valid values: <ul style="list-style-type: none"> • 0 (false) • 1 (true) |

| Parameter | Value type | Description |
|---------------------|------------|--|
| KerberosConfigName | String | |
| name | String | Required. The datasource to be updated. |
| newName | String | Defines a new name for the datasource. The new name must be unique for a datasource on the system. |
| password | String | The password for the account identified by the user parameter. If defined, the user parameter must also be used. |
| port | Integer | The port number of the datasource. |
| region | String | For AWS only. For valid values, call update_datasource_by_name from the command line with --help=true. |
| savePassword | Boolean | If enabled, savePassword saves and encrypts authentication credentials on the Guardium system. This is required when defining a datasource with an application that runs as a scheduled task (as opposed to on demand). When set to 1, the user and password parameters are required.
Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| secretName | String | |
| serviceName | String | For an Oracle datasource, the service name. |
| severity | String | Severity classification (or impact level) for the datasource.
For valid values, call update_datasource_by_name from the command line with --help=true. |
| shared | String | If set to true, share the datasource with other applications. To share the datasource with other users, assign roles from the GUI.
Valid values: <ul style="list-style-type: none">• Shared• Not Shared• true• false |
| useExternalPassword | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| useKerberos | Boolean | If set to 1, use Kerberos authentication. When set to 1, the KerberosConfigName is required.
Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| useLDAP | Boolean | If set to 1, use LDAP.
Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| user | String | The user name for the datasource. If defined, the password parameter must also be used. |
| useSSL | Boolean | If set to 1, use SSL authentication.
Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| walletZip | String | |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>.
IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

Use this command to change the datasource name from chickenDB2 to chicken_DB2:

```
grdapi update_datasource_by_name name=chickenDB2 newName="chicken_DB2"
```

update_datasource_credentials_in_group

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/datasource_group
```

GuardAPI syntax

```
update_datasource_credentials_in_group parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
| groupName | String | Required. |
| password | String | Required. |
| userName | String | |

update_datasource_custom_property

Use this command to update the associated values of a datasource custom property.

This API is available in Guardium V11.4 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/datasource_custom_prop
```

GuardAPI syntax

```
update_datasource_custom_property parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| addValues | String | The values that are to be added to the custom property. |
| deleteValues | String | The values that are to be deleted from the custom property. |
| name | String | Required. The name of the custom property. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

The following example deletes the value "Retail" from the custom property "Business Unit":

```
grdapi update_datasource_custom_property name="Business Unit" deleteValues="Retail"
```

The following example adds the value "Trading" to the custom property "Business Unit":

```
grdapi update_datasource_custom_property name="Business Unit" addValues="Trading"
```

Related concepts

- [Datasource APIs](#)

update_datasource_group

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/datasource_group
```

GuardAPI syntax

```
update_datasource_group parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------------|------------|--|
| appTypeCriteria | String | For valid values, call <code>update_datasource_group</code> from the command line with <code>--help=true</code> . |
| customPropsCriteria | String | A list of datasource custom properties on which to filter datasources that belong to the group. |
| dbTypeCriteria | String | For valid values, call <code>update_datasource_group</code> from the command line with <code>--help=true</code> . |
| groupName | String | Required. |
| groupType | String | Valid values: <ul style="list-style-type: none">• <i>DYNAMIC</i>• <i>STATIC</i> |
| hostCriteria | String | Host name criteria on which to filter datasources for this group. |
| newGroupName | String | |
| severityCriteria | String | Valid values: <ul style="list-style-type: none">• <i>ALL</i>• <i>INFO</i>• <i>NONE</i>• <i>LOW</i>• <i>MED</i>• <i>HIGH</i> |
| userCriteria | String | User name criteria on which to filter datasources for this group. |

update_engine_config

Use the `update_engine_config` command to change inspection engine settings.

An inspection engine monitors the traffic between servers and clients by using a specific database protocol (such as Oracle or Sybase). Configure an inspection engine from the Inspection Engine Configuration page. After the inspection engine is configured, you can use the `update_engine_config` command to change the parameters. For more information, see [Configuring inspection engines](#).

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/engine_config
```

GuardAPI syntax

```
update_engine_config parameter=value
```

Parameters

See [Inspection Engine Configuration](#) for details about each parameter.

| Parameter | Value type | Description |
|-------------------|------------|--|
| computeAverage | Boolean | When enabled, for each SQL construct logged, the average response time is computed. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| defaultAutoCommit | Boolean | Due to various auto-commit models for different databases, this value is used by Replay function to explicitly mark up the transactions and auto commit after each command. When enabled, commits and rollbacks are ignored. Databases currently supported include DB2®, Informix®, and Oracle. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |

| Parameter | Value type | Description |
|-----------------|------------|--|
| defaultCapture | Boolean | Used by Replay function to distinguish between transactions and capture values, meaning that if you have a prepared statement, assigned values are captured and replayed. Enable this if you want to replay your captured prepared statements as prepared statements. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| excludePorts | String | A list of ports to be ignored. Add values to this list if you know your database servers are processing non-database protocols, and you don't want Guardium® to waste cycles analyzing non-database traffic. For example, if you know the host on which your database resides also runs an HTTP server on port 80, you can add 80 to the ignored ports list, ensuring that Guardium does not process these streams. Separate multiple values with commas, and use a hyphen to specify an inclusive range of ports. For example: 101,105,110-223 |
| granularity | Integer | The number of minutes in a logging unit. If requested in a report, Guardium summarizes request data at this granularity. For example, if the logging granularity is 60, and a certain request occurred "n" times in a given hour. If disabled, the exact time when the command occurred within the hour is not recorded. But, if a rule in a policy is triggered by a request, a real time alert can indicate the exact time. When you define exception rules for a policy, those rules can also apply to the logging unit. For example, you might want to ignore 5 login failures per hour, but send an alert on the sixth login failure. Valid values: <ul style="list-style-type: none">• 1• 2• 5• 10• 15• 30• 60 |
| inspectData | Boolean | When enabled, data returned by SQL requests are inspected, and the ingress and egress counts are updated. If rules are used in the security policy, this parameter must be enabled. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| logExceptionSql | Boolean | If enabled, when exceptions are logged, the entire SQL statement is logged. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| logRecords | Boolean | When enabled, the number of records affected is recorded for each SQL statement (when applicable). Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) <p>Default = 0</p> <p>The records affected option is a sniffer operation which requires sniffer to process additional response packets and postpone logging of impacted data. This increases the buffer size and might potentially have an adverse effect on overall sniffer performance. Significant impact comes from really large responses. To prevent large amount of overhead associated with this operation, Guardium uses a set of default thresholds that allows sniffer to decide to skip processing operation when exceeded.</p> <p>Refer to Configuration and Control CLI Commands store max_results_set_size, store max_result_set_packet_size and store max_tds_response_packets, to set levels of granularity.</p> <p>Records Affected feature is not supported for:</p> <ul style="list-style-type: none">• DB2 when streaming is used to send the results.• AWS• Couchbase• Hadoop integration <p>Example of result set values:</p> <ul style="list-style-type: none">• Case 1, record affected value, positive number. This represents correct size of the result set.• Case 2, record affected value, -2. This means number of records exceeded configurable limit (This can be tuned through CLI commands).• Case 3, record affected value, -1. This shows any unsupported cases of packets configurations by Guardium.• Case 4, record affected value, -2. If the result set is sent by streaming mode.• Case 5, record affected value, less than -2. Intermediate result during record count to update user about current value, ends up with positive number of total records. For example, the server returns 1000 records in 4 packets:<ul style="list-style-type: none">◦ Packet #1 250◦ Packet #2 200◦ Packet #3 250◦ Packet #4 200 <p>Then records affected are reported as</p> <ul style="list-style-type: none">◦ Packet #1 -250◦ Packet #2 -500◦ Packet #3 -750◦ Packet #4 1000 |

| Parameter | Value type | Description |
|-----------------|------------|---|
| logSequencing | Boolean | When enabled, a record is made of the immediately previous SQL statement, as well as the current SQL statement, provided that the previous construct occurs within a short enough time period. Valid values: <ul style="list-style-type: none"> • 0 (false) • 1 (true) |
| maxHits | Integer | When returned data is being inspected, indicate how many hits (policy rule violations) are to be recorded. |
| parseXml | Boolean | The Inspection Engine does not normally parse XML traffic. Enable to parse XML traffic. Valid values: <ul style="list-style-type: none"> • 0 (false) • 1 (true) |
| recordEmpty | Boolean | When enabled, sessions containing no SQL statements are logged. When disabled, these sessions are ignored. Valid values: <ul style="list-style-type: none"> • 0 (false) • 1 (true) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

The following GuardAPI example changes three inspection engine parameters.

```
grdapi update_engine_config defaultCapture=true logExceptionSql=false maxHits=32
```

If successful, the command returns the following information:

```
ID=0
ok
```

Related concepts

- [Network mirroring methods \(SPAN, N-TAP\) and related inspection engines](#)

update_entry_location

This command updates the specified catalog entry if you specify a file name. If you do not specify a file name, this command updates the archive locations for the specified path and hostname.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/entry_location
```

GuardAPI syntax

```
update_entry_location parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|--|
| fileName | String | Identifies a single catalog entry to update. If omitted, all catalog entries on the specified hostname and path are updated. |
| hostName | String | Required. The hostname or IP address. |
| newHostName | String | A new hostname or IP address for the catalog entries. |
| newPath | String | A new path for the catalog entries. |
| password | String | The user's password. |

| Parameter | Value type | Description |
|-----------------|------------|---|
| path | String | Required. The path to the archive directory. <ul style="list-style-type: none"> Amazon S3: bucket name IBM COS: bucket name EMC Centera: Centera clipID FTP: Specify the directory relative to the FTP account home directory. SCP: Specify the directory as an absolute path. IBM Cloud: Container TSM: path |
| retention | Integer | The number of days to keep the entry in the catalog.
Default = 365 |
| storageSystem | String | Required. The type of archive storage system.
For valid values, call update_entry_location from the command line with --help=true. |
| user | String | The user account to access the host. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> all_managed: execute on all managed units but not the central manager all: execute on all managed units and the central manager group:<group name>: execute on all managed units identified by <group name> host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GuardAPI example

```
grdapi update_entry_location
fileName=a1.corp.com-1_4_2008-01-10_10:27:24.res.70.tar.gz.enc path=/mnt/nfs/ogazit/archive_results/ hostName=qaserver
storageSystem=SCP newPath=/var/dump/mojgan newHostName=192.168.1.18
```

Related tasks

- [Data and Result catalogs](#)

Related reference

- [Archive, export, import, purge, and restore APIs](#)
- [Catalog entry APIs](#)

update_external_stap_config

Use this API to modify External S-TAPs on a specified Guardium® host.

External S-TAPs are supported on UNIX or Linux machines only.

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/external_stap_config
```

GuardAPI syntax

```
update_external_stap_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------|------------|--|
| stapHost | String | Required. One of the following: <ul style="list-style-type: none"> The UUID of the External S-TAP®. <code>all_active</code>: All External S-TAPs that are configured to report to this Guardium system. For valid values, call update_external_stap_config from the command line with --help=true. |
| updateValue | String | Required. Modifiable parameters in the <code>guard_tap.ini</code> configuration file. For valid values of each parameter refer to the parameter descriptions in the Windows and UNIX-Linux S-TAP configuration. |

| Parameter | Value type | Description |
|-----------|------------|--|
| | | <p>TAP section:</p> <ul style="list-style-type: none"> • <i>add_to_verification_schedule</i> • <i>all_can_control</i> • <i>alternate_ips</i> • <i>appserver_installed</i> • <i>appserver_login_pattern</i> • <i>appserver_ports</i> • <i>appserver_session_pattern</i> • <i>appserver_session_postfix</i> • <i>appserver_session_prefix</i> • <i>appserver_username_postfix</i> • <i>appserver_username_prefix</i> • <i>appserver_usersess_pattern</i> • <i>appserver_usersess_postfix</i> • <i>appserver_usersess_prefix</i> • <i>bad_alloc_counter_max</i> • <i>buf_msg_time_interval</i> • <i>buffer_file_size</i> • <i>buffer_mmap_file</i> • <i>checksum</i> • <i>checksum_configuration</i> • <i>compression_level</i> • <i>connection_timeout_sec</i> • <i>db_exit_list</i> • <i>db_ignore_response</i> • <i>db_ignore_response_bypass_bytes</i> • <i>db_ignore_response_filter</i> • <i>db_ignore_response_resets_per_request</i> • <i>db_request_handler_enable</i> • <i>enable_dynamic_ring_buffers</i> • <i>extra_info</i> • <i>failover_tls</i> • <i>firewall_default_state</i> • <i>firewall_fail_close</i> • <i>firewall_force_unwatch</i> • <i>firewall_force_watch</i> • <i>firewall_installed</i> • <i>firewall_timeout</i> • <i>force_server_ip</i> • <i>guardium_ca_path</i> • <i>guardium_crl_path</i> • <i>kerberos_plugin_dir</i> • <i>load_balancer_ip</i> • <i>load_balancer_load_affinity</i> • <i>max_server_write_size</i> • <i>min_bytes_to_compress</i> • <i>modification_count</i> • <i>modification_host</i> • <i>modification_microsec</i> • <i>msg_aggregate_timeout</i> • <i>msg_count_watermark</i> • <i>participate_in_load_balancing</i> • <i>private_tap_ip</i> • <i>qrw_default_state</i> • <i>qrw_force_unwatch</i> • <i>qrw_force_watch</i> • <i>qrw_installed</i> • <i>remote_messages</i> • <i>sqlguard_cert_cn</i> • <i>stap_statistic</i> • <i>stap_statistic_version</i> • <i>syslog_messages</i> • <i>tap_buf_dir</i> • <i>tap_debug_output_level</i> • <i>tap_failover_session_quiesce</i> • <i>tap_failover_session_size</i> • <i>tap_identifier</i> • <i>tap_ip</i> • <i>tap_log_dir</i> • <i>upload_feature</i> <p>DB section:</p> <ul style="list-style-type: none"> • <i>connect_to_ip</i> • <i>db_user</i> • <i>db_version</i> • <i>exclude_networks</i> • <i>networks</i> |

| Parameter | Value type | Description |
|-----------------|------------|--|
| | | <ul style="list-style-type: none"> • <i>port_range_end</i> • <i>port_range_start</i> • <i>priority_count</i> • <i>real_db_port</i> <p>SQLGUARD section:</p> <ul style="list-style-type: none"> • <i>connection_pool_size</i> • <i>num_main_thread</i> • <i>sqlguard_ip</i> <p>SQLC_n section (UNIX Oracle Unified Auditing only):</p> <ul style="list-style-type: none"> • <i>instance</i> • <i>username</i> |
| api_target_host | String | <p>Required when running on a central manager.</p> <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • <i>all_managed</i>: execute on all managed units but not the central manager • <i>all</i>: execute on all managed units and the central manager • <i>group:<group name></i>: execute on all managed units identified by <i><group name></i> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <i>api_target_host=10.0.1.123</i>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <i>api_target_host=10.0.1.123</i>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GRDAPI examples

```
>grdapi update_external_stap_config stapHost=all-active updateValue=TAP.all_can_control:1
>grdapi update_external_stap_config stapHost=external_stap_uuid updateValue=TAP.all_can_control:1
>grdapi update_external_stap_config stapHost=all_active updateValue=TAP.all_can_control:1
```

Related reference

- [display_external_stap_config](#)
- [display_stap_config](#)
- [update_stap_config](#)

update_group_by_desc

This command updates the configuration of a group identified by its description.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/update_group_by_desc
```

GuardAPI syntax

```
update_group_by_desc parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| category | String | Update the category. A category is an optional label that is used to group policy violations and groups for reporting. |
| desc | String | Required. Identifies the group by its description. |
| GroupType | String | Update the group type. For a list of valid group types, see the type parameter of the create_group API. |

| Parameter | Value type | Description |
|------------------|------------|---|
| tuple_parameters | String | Required. Valid values: <ul style="list-style-type: none">• <i>client_ip</i>• <i>client_host_name</i>• <i>server_ip</i>• <i>server_host_name</i>• <i>source_program</i>• <i>db_name</i>• <i>db_user</i>• <i>os_user</i>• <i>db_type</i>• <i>net_protocol</i>• <i>server_port</i>• <i>sender_ip</i>• <i>analyzed_client_ip</i>• <i>incident</i> |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• <i>all_managed</i>: execute on all managed units but not the central manager• <i>all</i>: execute on all managed units and the central manager• <i>group:<group name></i>: execute on all managed units identified by <i><group name></i>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

Use this command to update the group named *A group* to use the group type *OBJECTS* and the category *New category*:

```
grdapic update_group_by_desc desc="A group" GroupType=OBJECTS category="New category"
```

Related reference

- [create_group](#)

update_group_by_id

This command updates the configuration of a group identified by its identification key.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/update_group_by_id
```

GuardAPI syntax

```
update_group_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|---|
| category | String | Update the category. A category is an optional label that is used to group policy violations and groups for reporting. |
| GroupType | String | Update the group type. For a list of valid group types, see the type parameter of the create_group API. |
| id | Integer | Required. Identifies the group by its identification key. |

| Parameter | Value type | Description |
|------------------|------------|---|
| tuple_parameters | String | Required. Valid values: <ul style="list-style-type: none">• <i>client_ip</i>• <i>client_host_name</i>• <i>server_ip</i>• <i>server_host_name</i>• <i>source_program</i>• <i>db_name</i>• <i>db_user</i>• <i>os_user</i>• <i>db_type</i>• <i>net_protocol</i>• <i>server_port</i>• <i>sender_ip</i>• <i>analyzed_client_ip</i>• <i>incident</i> |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• <i>all_managed</i>: execute on all managed units but not the central manager• <i>all</i>: execute on all managed units and the central manager• <i>group:<group name></i>: execute on all managed units identified by <i><group name></i>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

Use this command to update the group with identification key *100003* to use the group type *OBJECTS* and the category *New category*:

```
grdapi update_group_by_desc id=100003 GroupType=OBJECTS category="New category"
```

Related reference

- [create_group](#)

update_hashicorp_config

This command updates the HashiCorp configuration.

This API is available in Guardium v11.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/hashicorp
```

GuardAPI syntax

```
update_hashicorp_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------|------------|---|
| AuthType | String | For valid values, call <code>update_hashicorp_config</code> from the command line with <code>--help=true</code> . |
| name | String | Required. For valid values, call <code>update_hashicorp_config</code> from the command line with <code>--help=true</code> . |
| namespace | String | |
| password | String | The password. |
| username | String | The username. |
| useTLS | Boolean | Transport Layer Security (TLS) with server-side or client-side authentication.
Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| vaultHostName | String | The vault hostname. |

| Parameter | Value type | Description |
|-----------------|------------|------------------|
| vaultPortNumber | Integer | The port number. |

Example

The following example updates the username, authentication method, and port number.

```
grdapi update_hashicorp_config name="No TLS User and password API" username="newname" useTLS="true" vaultPortNumber="9999"
ID=1
ok
```

Related concepts

- [Datasource credential management APIs](#)

update_insights_agent_config

Update individual task manager parameters for Guardium® Insights.

Important: Do not change any of these parameters unless you are working with Guardium support. Some parameters are for informational purposes only and cannot be changed.

This API is available in Guardium v11.3 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/insights_agent_config
```

GuardAPI syntax

```
update_insights_agent_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|--|
| paramName | String | <p>Required. You can update the following parameters:</p> <ul style="list-style-type: none"> • ALLOW_ACTIVITY_INSIGHTS_POLICY_INSTALLATION - When set to 1 (on), creates a dedicated GuardiumInsightPolicy and supports blocking users from Guardium Insights. Default = 0 (off). • FORCE_SYNC - When set to 1 (on), forces the Insights agent to verify that the Insights-related setup is synced between the central manager and managed units. Default = 0 (off). Guardium Insights and Guardium Data Protection. • MAX_BLOCKING_TASK_WAIT_TIME - The maximum time (in seconds) that the task manager waits for "blocking tasks" to complete before moving on to process the next queued tasks. Default = 300 (seconds). Value is any integer 0 or greater. • MAX_CONSECUTIVE_ERROR_HANDLING – The number of error messages to send to Guardium Insights upon recurring failure executing the same task. Default = 1. Value is any integer 1 or greater. • MAX_CONCURRENT_TASK_THREADS - Number of concurrent tasks that the task manager can run. Default = 30. Value is any integer 1 or greater. • TASK_GENERATOR_EXECUTION_INTERVAL - The interval by which the internal task generator task is checking tasks to process when agent is not registered. Default = 10 (seconds). Value is any integer 5 or greater. • TASK_MANAGER_PARAM_LOAD_INTERVAL - The interval by which the task manager looks for parameter changes. Default = 10 (seconds). Value is any integer 5 or greater. • TASK_QUEUE_EXECUTION_INTERVAL - The interval by which the task manager checks the task queue. Default = 10 (seconds). Value is any integer 5 or greater. <p>Note: The following parameters display in get_insights_agent_config, but cannot be changed,</p> <ul style="list-style-type: none"> • EXCLUDED_GI_DATAMARTS - The list of data marts to exclude from the extraction profile. • MAX_GI_DATAMART_EXTRACTION_PROFILE_SUPPORTED - The name of the supported data mart extraction profile. |
| paramValue | String | Required. The new value for the paramName. |

Related reference

- [get_insights_agent_config](#)

update_insights_registration_config

This API allows you to update the Guardium® Insights registration information.

This API is available in Guardium v11.3 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/insights_registration
```

GuardAPI syntax

```
update_insights_registration_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|--|
| insights_apikey_token | String | Required. An API token that is generated from Guardium Insights to allow external sources to execute RESTAPI calls on Guardium Insights. The token includes the encrypted Guardium Insights tenant ID. |
| insights_ca_cert_cn | String | The Insights certificate common name that is generated when the certificate is created. During the registration process, you can specify the certificate common name to verify the CN field as part of the standard certificate exchange authentication. |

update_ip_restriction_allowlist

This command adds or removes IP addresses from an IP restriction allowlist.

You can create allowlists either from the GUI or by using the [enable_disable_ip_restriction](#) API. For more information, see [Managing access by IP address](#).

This API is available in Guardium V11.4 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/ip_restriction
```

GuardAPI syntax

```
update_ip_restriction_allowlist parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| action | String | Required. Specify whether to add or remove an IP address. Valid values: <ul style="list-style-type: none">• ADD• REMOVE |
| ips | String | Required. A list of one or more comma-separated IP addresses to add or remove. |
| type | String | Required. Specify whether to update the IP address allowlist for the GUI, for SSH, or both (ALL). Valid values: <ul style="list-style-type: none">• ALL - Both GUI and SSH• GUI• SSH |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group_name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

This example adds an IP address to the GUI allowlist.

```
>grdapi update_ip_restriction_allowlist action="ADD" ips="9.160.142.63" type="GUI"
```

Related reference

- [enable_disable_ip_restriction](#)
- [get_ip_restriction_config](#)

Related information

- [Managing access by IP address](#)

update_istap_config

Use this command to update the filtering settings on IBM i.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/istap_config
```

GuardAPI syntax

```
update_istap_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------------------|------------|--|
| check_server_hb | Boolean | Network connection check. Valid values: <ul style="list-style-type: none"> • 0 (false): Do not use failover. • 1 (true): Use failover. |
| connection_timeout_sec | String | Number of seconds after which theS-TAP® considers a Guardium® server to be unavailable. It can have any integer value. |
| datasourceName | String | Required. IP or name of the IBM i server. |
| filter_audit_entry_types | String | The specified QAUDJRN audit entry filter, if any. Specifies which audit journal entry types should be processed. The default is 'AD AF CA CO DO GD OM OR OW PG PW RA RO RZ SV ZC ZR' |
| filter_client_acct | String | The specified client accounting filter, if any. Only one client accounting filter can be specified. |
| filter_client_app | String | The specified client application filter, if any. Only one client application filter can be specified. |
| filter_client_program | String | The specified client program filter, if any. Only one client program filter can be specified. |
| filter_client_user | String | The specified client user filter, if any. Only one client user filter can be specified. |
| filter_client_wkstn | String | The specified client workstation filter, if any. Only one client workstation filter can be specified. |
| filter_job | String | The specified job filter, if any. Only one job name or generic job name can be specified. |
| filter_port | String | The specified port filter, if any. Only one port filter can be specified. Filtering by port is only supported in release 7.1 and later. |
| filter_rdb | String | The specified relational database filter, if any. Up to 10 relational database names can be specified. Filter_RDB is a case sensitive filter. Execute this command on your target database and enter the name exactly as it is returned. |
| filter_system_sql | String | The specified system SQL statement filter. Specifies whether system SQL statements should be audited (Y or N). The default is Y. |
| filter_table | String | The specified table filter, if any. Up to ten file names or generic file names can be specified. The specified library name must be the system schema name (10 character name). The file name can be either the system table name or table name (long or short name). |
| filter_tcpip | String | The specified TCP/IP filter, if any. Only one TCP/IP address can be specified. |
| filter_user | String | The specified user or group user profile filter, if any. Up to 10 usernames or generic usernames can be used.
Important: If you want to set the filter_user parameter value to null, then enter null in lowercase. If you enter NULL in uppercase, the system apply DBUser=NULL filter. |
| guardium_host | String | IP address or hostname of the Guardium system that acts as the host for the S-TAP. |
| prevent_skipped_entries | String | Directs the SQL auditing to handle the case where the audit server job is overwhelmed with detail. Valid values: <ul style="list-style-type: none"> • N • Y: The audit server is given preference over the performance of the work stream. Default = N |
| remote_messages | String | Send messages to the active Guardium host. Valid values: <ul style="list-style-type: none"> • 0: Do not send messages • 1: Send messages to the active Guardium system. |

| Parameter | Value type | Description |
|---------------|------------|---|
| start_monitor | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true): The auditing process starts (or restarts) on the i server after the configuration table is updated. When the auditing process is started, stored procedures on DB2 for i are invoked that: <ul style="list-style-type: none"> ◦ Create the message queue that will be used to send entries to the InfoSphere Guardium collector and starts a global database monitor using a view with an INSTEAD OF trigger (which sends the entries to the message queue) ◦ Start PASE and S-TAP. ◦ Receive journal entries from QAUDJRN and add them to the message queue. <p>Default = 1 (true)</p> |
| start_user | String | |

Examples

To start monitoring in the server named db21nn:

```
grdapi datasourceName=db21nn update_istap_config start_monitor=1
```

Related concepts

- [DB2 for IBM i S-TAP](#)

Related reference

- [S-TAP for IBM i APIs](#)

update_managed_units_ping_time

This API is available in Guardium v11.3 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/update_managed_units_ping_time
```

GuardAPI syntax

```
update_managed_units_ping_time parameter=value
```

update_policy

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/policy
```

GuardAPI syntax

```
update_policy parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------|------------|---|
| baselineDesc | String | |
| categoryName | String | For valid values, call <code>update_policy</code> from the command line with <code>--help=true</code> . |
| logFlat | Boolean | <p>Valid values:</p> <ul style="list-style-type: none"> • 0 (false) • 1 (true) |
| pattern | String | |
| policyDesc | String | Required. |
| policyLevel | String | |

| Parameter | Value type | Description |
|-----------------|------------|---|
| rulesOnFlat | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| securityPolicy | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

update_policy_analyzer_interval

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/update_policy_analyzer_interval
```

GuardAPI syntax

```
update_policy_analyzer_interval parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| interval | String | Valid interval values are 2 - 60. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

update_qr_action

This command updates an existing query rewrite action with a new name and optional description.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/qr_action
```

GuardAPI syntax

```
update_qr_action parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|---|
| actionName | String | Required. The unique name of the query rewrite action. |
| definitionName | String | Required. The query rewrite definition that is associated with this action. |
| description | String | Textual description of the action. |
| newName | String | The new name for this action. |

Examples

To rename qr action2 to new qr action2:

```
grdapi update_qr_action definitionName="case 2" actionName="qr action2" newName="new qr action2"
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

update_qr_add_where_by_id

This command updates an existing "add where" function with new text.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/update_qr_add_where_by_id
```

GuardAPI syntax

```
update_qr_add_where_by_id parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------|------------|---|
| addQualifierFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| qrAddWhereId | Long | Required. The unique identifier for the query rewrite "add where" function. |
| whereText | String | The replacement text for the specified where clause. |

Examples

```
grdapi update_qr_add_where_by_id qrAddWhereId=22222 whereText="1=2"
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

update_qr_condition

This command creates a query rewrite condition.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/qr_condition
```

GuardAPI syntax

```
update_qr_condition parameter=value
```

Parameters

| Parameter | Value type | Description |
|---------------------|------------|--|
| conditionName | String | Required. The unique name of this query rewrite condition. |
| definitionName | String | Required. The query rewrite definition that is associated with this condition. |
| depth | Integer | The depth of the parsed SQL that this condition applies to (1 and higher). The value 1 means that the query rewrite condition applies to any matching SQL at any depth. Default = 1 |
| isForAllRuleObjects | Boolean | Indicates that the specified condition applies to all objects for the fired rule. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 |
| isForAllRuleVerbs | Boolean | Whether or not the specified condition applies to all verbs for the fired rule. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 |
| isObjectRegex | Boolean | Whether or not the specified object is specified by using a regular expression. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 |
| isVerbRegex | Boolean | Whether or not the specified verb is specified by using a regular expression. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 |
| newName | String | The new name for the query rewrite condition. |
| object | String | An object (table or view). The default "*" means all objects. This can also be specified as a regular expression, in which case set the isVerbRegex to True. |
| order | Integer | Specifies the order in which to assemble multiple related query rewrite conditions for complex SQL. Default = 1. |
| verb | String | A verb (select, insert, update, delete). The default "*" means all verbs. |

Examples

```
grdapi update_qr_condition definitionName="case 16" conditionName="qr_cond15_3" newName="qr_cond16_3" verb=select object=* dept=2 order=3
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

update_qr_definition

This command updates an existing query rewrite definition.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/qr_definition
```

GuardAPI syntax

```
update_qr_definition parameter=value
```

Parameters

| Parameter | Value type | Description |
|----------------|------------|--|
| dataBaseType | String | Required. The type of database this query rewrite definition is associated with. For valid values, call update_qr_definition from the command line with --help=true. |
| definitionName | String | Required. A unique name for this query rewrite definition condition. |
| description | String | Textual description |
| isNegateQrCond | Boolean | Specify if there is a NOT flag on the set of query rewrite conditions that are associated with this definition. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| newName | String | Specifies a new unique name. |
| sampleSql | String | Specifies a sample SQL statement. In most cases, you will not use this unless you want to use the inputted sample SQL later in the UI. |

Examples

```
grdapi update_qr_definition DataBaseType="DB2" definitionName="case 15" sampleSql="select EMPNO from EMP where ENAME = (select ENAME from EMP where SAL = (select SAL from EMP where HIREDATE = to_date('06/09/1981 00:00:00', 'MM/DD/YYYY HH24:MI:SS')))" newName="DB2_case 15"
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

update_qr_replace_element_byId

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/update_qr_replace_elementById
```

GuardAPI syntax

```
update_qr_replace_elementById parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------------|------------|--|
| columnAlias | String | Specify an alias for a column name. For more information, see Starting the IBM Knowledge Catalog and Guardium Data Protection integration . |
| isFromAllRuleElements | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| isFromRegex | Boolean | Whether or not the "from" element is specified by using a regular expression. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 |
| isReplaceToFunction | Boolean | Whether or not the "replace to" is the name of a function, such as user-defined function. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| qrReplaceElementId | Long | Required. The unique ID of the query rewrite action. |
| replaceFrom | String | The incoming string for a matching rule that is to be replaced. Use replaceType to indicate specifically which element of the incoming query to examine. |

| Parameter | Value type | Description |
|-----------|------------|--|
| replaceTo | String | The replacement string for the matching element. |

Examples

```
grdapi update_qr_replace_element_byId qrReplaceElementId=1 isFromAllRuleElements=false isFromRegex=false
isReplaceToFunction=false replaceFrom=emp replaceTo=NEW_EMP_UPDATED
```

Related concepts

- [Query rewrite](#)

Related reference

- [Query rewrite APIs](#)

update_quarantine_allowed_until

This command updates parameters to prevent a user from logging in after a specified length of time passes.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/quarantine_allowed_until
```

GuardAPI syntax

```
update_quarantine_allowed_until parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| allowedUntil | String | Required. The date and time to begin the quarantine in one of the following formats: <ul style="list-style-type: none"> • YYYY-MM-DD hh:mm:ss • A relative time (such as NOW +1 HOUR) For more information about relative time, see Relative to NOW . |
| dbUser | String | Required. The name of the database user to quarantine. |
| serverIp | String | Required. The server IP address. |
| serviceName | String | Required. The server name. |
| type | String | Required. If the database is not IBM Z® or IMS, specify <i>normal</i> . Valid values: <ul style="list-style-type: none"> • <i>normal</i> • <i>DB2Z</i> • <i>IMS</i> |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> • <i>all_managed</i>: execute on all managed units but not the central manager • <i>all</i>: execute on all managed units and the central manager • <i>group:<group name></i>: execute on all managed units identified by <i><group name></i> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <i>api_target_host=10.0.1.123</i>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <i>api_target_host=10.0.1.123</i>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GuardAPI example

The following command updates the time to start the quarantine for this user:

```
grdapi update_quarantine_allowed_until allowedUntil="NOW +2 HOUR" dbUser="Hadrian.Swall" serverIp="9.32.0.255"
serviceName="company.ibm.com" type="normal"
```

Related concepts

- [Dates and Timestamps](#)
- [Logging or ignoring rule actions](#)

Related reference

- [create_quarantine_allowed_until](#)

update_quarantine_until

This command updates the parameters that prevent a user from logging for a specified length of time.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/quarantine_until
```

GuardAPI syntax

```
update_quarantine_until parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| dbUser | String | Required. The name of the database user to quarantine. |
| quarantineUntil | String | Required. The date and time to end the quarantine in one of the following formats: <ul style="list-style-type: none"> • YYYY-MM-DD hh:mm:ss • A relative time (such as NOW +1 HOUR) For more information about relative time, see Relative to NOW . |
| serverIp | String | Required. The server IP address. |
| serviceName | String | Required. The server name. |
| type | String | Required. If the database is not IBM Z® or IMS, specify <i>normal</i> . Valid values: <ul style="list-style-type: none"> • <i>normal</i> • <i>DB2Z</i> • <i>IMS</i> |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none"> • <i>all_managed</i>: execute on all managed units but not the central manager • <i>all</i>: execute on all managed units and the central manager • <i>group:<group name></i>: execute on all managed units identified by <i><group name></i> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GuardAPI example

The following command changes the quarantine for this user from 1 hour to 2 hours after the command is called:

```
grdapi create_quarantine_until quarantineUntil="NOW +2 HOUR" dbUser="Hadrian.Swall" serverIp="9.32.0.255"
serviceName="company.ibm.com" type="normal"
```

Related concepts

- [Dates and Timestamps](#)
- [Logging or ignoring rule actions](#)

Related reference

- [create_quarantine_until](#)

update_ranger_config

This API updates the configuration parameters for the Ranger integration.

This command requires valid administrative authority on the Ambari server such as an admin or service administrator account. After running the command, the Ambari administrator must restart the affected Hadoop components so that the changes take effect.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/update_ranger_config
```

GuardAPI syntax

```
update_ranger_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| clusterName | String | Required. Ambari cluster name. |
| hostname | String | Required. Hostname or IP address of the Ambari server. |
| newClusterName | String | New cluster name for this ranger configuration. |
| password | String | Required. Password for the admin user specified by <code>user_name</code> |
| port | Integer | Port on the Ambari server for the user interface. |
| sslEnabled | Boolean | Sets whether SSL is enabled for communication with this Ranger. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false) |
| user_name | String | Required. Ambari server username; must be an admin or service admin user. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To change the cluster name of this ranger configuration to Cluster4:

```
grdapi update_ranger_config hostname=hw-cl4-05 user_name=admin port=8080 password=xxxxxx clusterName=Cluster4
```

Sample output:

```
ID=0
Configuration for Cluster: Cluster4
Updated.
admin@hw-cl4-05:8080 Cluster4
```

Related concepts

- [Hadoop integration using Hortonworks and Apache Ranger](#)

Related reference

- [Hadoop monitoring APIs](#)
- [S-TAP Hadoop parameters](#)

update_ranger_hdfs_config

Use this command to update a Hadoop integration with Ranger HDFS that send data to the specified S-TAP.

This API is available in Guardium V11.3 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/update_ranger_hdfs_config
```

GuardAPI syntax

```
update_ranger_hdfs_config parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------------------|------------|---|
| ldLibraryPath | String | Locate libjvm.so (for example, /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.191.b12-1.el7_6.x86_64/jre/lib/amd64/server/libjvm.so) and set <code>ld_library_paths</code> to the directory that contains libjvm.so (for example, /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.191.b12-1.el7_6.x86_64/jre/lib/amd64/server). |
| principal | String | Required for Kerberos. The value of Ranger HDFS user. |
| rangerHDFSAuditHistoryLength | Integer | Required. |
| rangerHdfsAuditDirs | String | Comma-separated list of directories where Ranger logs the service audits. Include one directory that contains the daily log directories, for each service you want to monitor. Usually the paths are located under /ranger/audit.

Example service directories for CDP 7: /ranger/audit/hive/hiveServer2,/ranger/audit/kafka/kafka,/ranger/audit/hbase/hbaseMaster,/ranger/audit/hbase/hbaseRegional,/ranger/audit/atlas/atlas,/ranger/audit/hdfs/hdfs

Example service directories for HW 3: /ranger/audit/hbaseMaster,/ranger/audit/hbaseRegional,/ranger/audit/hdfs,/ranger/audit/hiveServer2,/ranger/audit/kafka,/ranger/audit/solr,/ranger/audit/storm |
| rangerHdfsKeytab | String | Required for Kerberos. Location of the Kerberos keytab that contains the principal used to connect to HDFS. |
| rangerHdfsLibLocation | String | Locate libhdfs.so provided by Hadoop cluster (for example, /usr/hdp/3.1.0.141-1/usr/lib/libhdfs.so) and set <code>ranger_hdfs_lib_location</code> to the directory that contains libhdfs.so (for example, /usr/hdp/3.1.0.141-1/usr/lib). |
| rangerHdfsNameNode | String | IP or hostname of the HDFS NameNode. |
| rangerHdfsPollMs | Integer | Time interval, in milliseconds, the S-TAP® waits between checking for new Ranger audits in HDFS. |
| rangerHdfsPort | Integer | The HDFS NameNode port the S-TAP connects to. |
| rangerHdfsUser | String | The user with which S-TAP connects to HDFS. If the HDFS setup is using Kerberos, set the parameter to the Kerberos principal. |
| sTapHostName | String | Required. Host name or IP of the S-TAP that receives the Ranger audit messages from the Ranger. |
| useKerberos | Boolean | Enables Kerberos authentication for this connection. When enabled, requires values for Principal and Ranger HDFS keytab. Valid values: <ul style="list-style-type: none">• 0: Disabled• 1: Enabled Default = 0 |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Related concepts

- [Hadoop integration using Ranger HDFS for Hortonworks and Cloudera 7](#)

Related reference

- [Hadoop monitoring APIs](#)
- [S-TAP Hadoop parameters](#)

update_ranger_service

Use this command to update the Ranger service that is mapped to an S-TAP®.

This command requires valid administrative authority on the Ambari server such as an admin or service administrator account. After running the command, the Ambari administrator must restart the affected Hadoop components so that the changes take effect.

This API is available in Guardium V10.1.4 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/update_ranger_service
```

GuardAPI syntax

```
update_ranger_service parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| clusterName | String | Required. Ambari cluster name. |
| port | Integer | Port on the Ambari server for monitoring. |
| serviceName | String | Required. Name of the service. Valid values: <ul style="list-style-type: none">• hdfs• hive• hbase• kafka• solr• storm |
| stapHostName | String | Required. Host name or IP of the S-TAP that receives the log4j audit messages from the Ranger. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

To change the port for this ranger to 5534:

```
grdapi update_ranger_service clusterName=Cluster4 serviceName=HDFS stapHostName=<Guardium host> port=5534
```

Sample output:

```
ID=0
The Hadoop service configuration has been changed. Ask the Hadoop administrator to restart the Hadoop service to activate the changes.
HDFS Monitoring Enabled on <Guardium host>:5534
Note: Only one port can be configured per S-TAP host. Changing the port here will update it automatically for all Hadoop services configured to this S-TAP.
```

Related concepts

- [Hadoop integration using Hortonworks and Apache Ranger](#)

Related reference

- [Hadoop monitoring APIs](#)
- [S-TAP Hadoop parameters](#)

update_rule

This command updates a policy rule.

This command updates the parameters that you specify for an existing rule in a specified policy. Only the rule name (*ruleDesc*) and policy name (*fromPolicy*) are required. If you do not specify a rule field, the field is ignored and not changed.

For more information about rule fields, see [Rule definition fields](#).

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/update_rule
```

GuardAPI syntax

```
update_rule parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------------|------------|---|
| analyzedClientIP | String | |
| analyzedClientIPGroup | String | |
| analyzedClientIPNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| analyzedClientNetMask | String | |
| appEventDate | String | Application event date. |
| appEventExists | Boolean | Match for an application event only. Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| appEventNumValue | String | Application event number value. |
| appEventStrGroup | String | Application string group. |
| appEventStrValue | String | Application string value. |
| appUserGroup | String | Application user group. |
| appUserName | String | Application username. |
| appUserNameNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| audit | String | Audit name. |
| authType | String | |
| authTypeGroup | String | |
| authTypeNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true)
Default = 1 (true) |
| category | String | Report category. For valid values, call update_rule from the command line with --help=true. |
| cicsUserGroup | String | CICS user group name. |
| cicsUserId | String | CICS user ID. |
| classification | String | Classification name. |
| clientHostGroup | String | Client host group name. |
| clientHostName | String | Client hostname. |
| clientHostNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| clientInfo | String | Client information. Use for Db2 and DB2_COLLECTION_PROFILE. |
| clientInfoGroup | String | Client information group. Use for DB2_COLLECTION_PROFILE. |
| clientIP | String | |
| clientIpGroup | String | |
| clientIpNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| clientMac | String | |

| Parameter | Value type | Description |
|--|------------|--|
| clientMacNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| clientNetMask | String | |
| clientOsName | String | |
| clientOsNameGroup | String | |
| clientOsNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| clientProgramUserServerInstanceGroup | String | |
| clientProgramUserServerInstanceNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| clientProgramUserServerInstanceOsDbGroup | String | |
| clientProgramUserServerInstanceOsDbNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| clientTimezone | String | |
| clientTimezoneGroup | String | |
| clientTimezoneNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true)
Default = 1 (true) |
| command | String | |
| commandGroupAndFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| commandNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| commandsGroup | String | |
| continueToNext | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| dataPattern | String | |
| datasetType | String | |
| dateTime | String | Date and time (Time period parameter) |
| dbName | String | Database name. |
| dbNameGroup | String | Database group name. |
| dbNameNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| dbnameObjectGroup | String | Database object group name. |
| dbnameObjectGroupNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| dbProtocol | String | |
| dbProtocolGroup | String | |

| Parameter | Value type | Description |
|-------------------------------------|------------|--|
| dbProtocolNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| dbType | String | Database type. |
| dbTypeGroup | String | |
| dbTypeNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| dbUser | String | Database username. |
| dbUserGroup | String | Database user group. |
| dbUserNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| ddName | String | |
| dliCallCodes | String | |
| errorCode | String | An error code. |
| errorCodeNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| errorGroup | String | |
| eventType | String | |
| eventUserName | String | |
| exceptionType | String | An exception type. |
| exceptionTypeIdNo ^t Flag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| failureCode | Integer | A numeric failure code. |
| failureCodeGroup | String | The group for a failure code. |
| failureCodeNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| fieldGroupAndFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| fieldName | String | |
| fieldNameGroup | String | |
| fieldNameNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| fileGroup | String | |
| fileId | String | |
| fromPolicy | String | Required. The name of this policy. |
| functionCode | String | |
| functionCodeGroup | String | |
| imsDefinitionName | String | |
| incident | String | |
| label | String | |
| labelNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true)
Default = 1 (true) |
| literal | String | |
| literalAndFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true)
Default = 1 (true) |
| literalGroup | String | |

| Parameter | Value type | Description |
|--------------------------|------------|---|
| literalNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| logFlag | String | The log flag. Corresponds to Record Values parameter. |
| magenAddToHistory | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| magenPageUrl | String | |
| magenPageUrlGroup | String | |
| magenPageUrlNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| maskingPattern | String | |
| matchedReturnedThreshold | Integer | |
| messageTemplate | String | |
| minCount | Integer | |
| netProtocol | String | |
| netProtocolGroup | String | |
| netProtocolNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| newDesc | String | A new description for this rule. |
| objectCommandGroup | String | |
| objectCommandNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| objectFieldGroup | String | |
| objectFieldNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| objectGroup | String | |
| objectGroupAndFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| objectName | String | |
| objectNameNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| osUser | String | Operating system user. |
| osUserGroup | String | Operating system user group. |
| osUserNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| pattern | String | |
| programGroup | String | The program group. |
| programId | String | The program ID. |
| quarantineMinutes | Integer | |
| recordRuleDescription | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| recordsAffectedThreshold | Integer | |
| regionGroup | String | |
| regionId | String | |

| Parameter | Value type | Description |
|---------------------------|------------|---|
| replacementChar | String | |
| resetInterval | Integer | |
| responseLengthThreshold | Long | |
| ruleDesc | String | Required. The name of the rule to update. To update the rule description, use the <i>newDesc</i> parameter. |
| senderIP | String | |
| senderIPGroup | String | |
| senderIPNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| senderNetMask | String | |
| serverDescription | String | |
| serverDescriptionGroup | String | |
| serverDescriptionNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| serverHostGroup | String | Server host group. |
| serverHostName | String | Server hostname. |
| serverHostNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| serverIP | String | The server IP. |
| serverIpGroup | String | Server IP group. |
| serverIpNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| serverNetMask | String | |
| serverOsName | String | |
| serverOsNameGroup | String | |
| serverOsNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| serverPort | Integer | |
| serverPortGroup | String | |
| serverPortNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| serviceName | String | |
| serviceNameGroup | String | |
| serviceNameNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| serviceObjectGroup | String | |
| serviceObjectGroupNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| session | String | Required. Valid values: <ul style="list-style-type: none">• LOCAL• TAP_DECRYPTED• ENCRYPTED |
| sessionNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |

| Parameter | Value type | Description |
|-----------------------|------------|---|
| severity | String | The alert severity. Can be one of: <ul style="list-style-type: none">• Info• Low• None• Med• High |
| slpFieldAndFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| slpFieldGroup | String | |
| slpFieldName | String | |
| slpFieldNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| sourceProgram | String | |
| sourceProgramGroup | String | |
| sourceProgramNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| sqlPattern | String | |
| startTime | String | |
| startTimeNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| terminalGroup | String | |
| terminalId | String | |
| transactionGroup | String | |
| transactionId | String | |
| triggerOncePerSession | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| tuplesDesc | String | |
| tuplesGroup | String | |
| tuplesNotFlag | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) |
| xmlPattern | String | A regular expression (regex) to match. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

GuardAPI example

```
grdapic update_rule ruleDesc="Rule Description" fromPolicy="policy1" serviceName="ANY"
```

Related reference

- [Rule definition fields](#)

update_shared_secret

Use this API to update the shared secret for a central manager and its associated managed units. This API is only available as a grdapi.

Be sure to run **update_shared_secret** from a central manager.

Set the shared secret before you register the central manager and managed units. For more information, see [Registering units](#).

When you update the shared secret from the central manager, the secret is propagated from the central managed to all associated managed units that are available. An error message is returned if a managed unit is offline or not available.

Note: The central manager and all managed units must be on the same Guardium version.

This API is available in Guardium v11.4 and later.

GuardAPI syntax

```
update_shared_secret parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| enable | Boolean | Required. When <i>enable</i> is set to 1, Guardium® follows strong password rules for the shared secret. That is, the value of <i>SharedSecret</i> must be a minimum of 15 characters, and follow the rules that are described in store_password_validation .
Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 0 (false)
Note: While SharedSecret uses the strong password rules, the shared secret is not related to passwords. |
| SharedSecret | String | A shared secret that allows communication between the central manager and associated managed units. |
| api_target_host | String | Specifies the target hosts where the API executes. Valid values: <ul style="list-style-type: none">• all_managed: execute on all managed units but not the central manager• all: execute on all managed units and the central manager• group:<group name>: execute on all managed units identified by <group name>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, api_target_host=10.0.1.123.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, api_target_host=10.0.1.123. IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode. |

Examples

The following example shows the shared secret with strong password rules enabled. In addition, only the available managed units are updated.

```
grdapi update_shared_secret SharedSecret="!QertyqUerty!1029" enable=true  
ID=0  
The following managed unit was offline: sys-vm01.my.company.com.  
The offline unit(s) will not be updated  
Updating managed unit : sys-vm03.my.company.com.  
Updating managed unit : sys-vm04.my.company.com.
```

update_stap_config

Modifies the configuration of the S-TAPs reporting to the specified Guardium® systems.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/stap_config
```

GuardAPI syntax

Use the *updateValue* parameter to modify the listed parameters in the file *guard_tap.ini*. Each listed parameter indicates if it is relevant for Windows or Unix. You can specify any combination of parameters in this command.

```
update_stap_config parameter=value updateValue=<guard_tap.ini section name>.〈parameter〉:value
```

To modify multiple parameters:

```
update_stap_config parameter=value updateValue=<guard_tap.ini section name>.<parameter>:value&<guard_tap.ini section name>.<parameter>:value...
```

Parameters

CAUTION:

Many of these parameters are advanced and are usually only modified by IBM Technical Support.

| Parameter | Value type | Description |
|----------------|------------|---|
| stapHost | String | <p>Required. The host name or IP address of a database server on which Guardium system, or a comma-separated list of host names or IP addresses, or one of:</p> <ul style="list-style-type: none">• 9.70.147.80• all_active: All S-TAPs that are configured to report to this Guardium system• all_unix_active: All S-TAPs that are configured to report to this Guardium system and are running on UNIX servers.• all_windows_active: All S-TAPs that are configured to report to this Guardium system and are running on Windows servers. <p>For valid values, call update_stap_config from the command line with --help=true.</p> |
| tap_identifier | NULL | Used to distinguish inspection engines from one another. If unspecified, Guardium auto-populates the field with a unique name using the database type and sequence number. |
| updateValue | String | <p>Required. Modifiable parameters in the guard_tap.ini configuration file. For valid values of each parameter refer to the parameter descriptions in the Windows and UNIX-Linux S-TAP® configuration.</p> <p>TAP section:</p> <ul style="list-style-type: none">• add_to_verification_schedule (UNIX, Windows)• alert_on_shared_memory_enabling (Windows)• all_can_control (UNIX, Windows)• alternate_ips (UNIX, Windows)• appserver_installed (UNIX, Windows)• appserver_login_pattern (UNIX, Windows)• appserver_ports (UNIX, Windows)• appserver_session_pattern (UNIX, Windows)• appserver_session_postfix (UNIX, Windows)• appserver_session_prefix (UNIX, Windows)• appserver_username_postfix (UNIX, Windows)• appserver_username_prefix (UNIX, Windows)• appserver_usersess_pattern (UNIX, Windows)• appserver_usersess_postfix (UNIX, Windows)• appserver_usersess_prefix (UNIX, Windows)• atap_exec_location (UNIX)• auto_discovery (Windows)• bad_alloc_counter_max (UNIX)• buf_msg_time_interval (UNIX, Windows)• buffer_file_size (UNIX, Windows)• buffer_mmap_file (UNIX, Windows)• buffer_percentage_for_priority_packet (UNIX)• cas_checkpoint_period (UNIX, Windows)• cas_client_baseline (UNIX, Windows)• cas_client_checkpoint (UNIX, Windows)• cas_fail_over_file (UNIX, Windows)• cas_fail_over_file_size_limit (Windows)• cas_max_reconnect_attempts (UNIX, Windows)• cas_md5_size_limit (UNIX, Windows)• cas_raw_data_limit (UNIX, Windows)• cas_reconnect_interval (UNIX, Windows)• cas_task_baseline (UNIX, Windows)• cas_task_checkpoint (UNIX, Windows)• cassandra_audit_delimiter (UNIX)• cassandra_audit_enabled (UNIX)• checksum (UNIX, Windows)• checksum_configuration (UNIX, Windows)• compression_level (UNIX, Windows)• connection_timeout_sec (UNIX, Windows, i)• correlation_timeout (Windows)• db_exit_list (UNIX)• db2_shmem_driver_installed (Windows)• db2_tap_installed (Windows)• db_ignore_response (UNIX, Windows)• db_ignore_response_bypass_bytes (UNIX, Windows)• db_ignore_response_filter (UNIX, Windows)• db_ignore_response_local (UNIX, Windows)• db_ignore_response_resets_per_request (UNIX, Windows)• db_request_handler_enable (UNIX)• devices (UNIX, Windows)• disable_shared_memory_if_turned_on (Windows)• discovery_debug (UNIX)• discovery_interval (UNIX, Windows). Valid values: <n>m (for minutes) and <n>h (for hours).• enable_dynamic_ring_buffers (UNIX)• extra_info (UNIX, Windows) |

| Parameter | Value type | Description |
|-----------|------------|---|
| | | <ul style="list-style-type: none"> • <i>failover_tls</i> (UNIX, Windows,i) • <i>fam_enable</i> (UNIX, Windows) • <i>firewall_default_state</i> (UNIX, Windows) • <i>firewall_fail_close</i> (UNIX, Windows) • <i>firewall_force_unwatch</i> (UNIX, Windows) • <i>firewall_force_watch</i> (UNIX, Windows) • <i>firewall_installed</i> (UNIX, Windows) • <i>firewall_timeout</i> (UNIX, Windows) • <i>force_server_ip</i> (UNIX) • <i>guardium_ca_path</i> (UNIX) • <i>guardium_crl_path</i> (UNIX) • <i>hunter_trace</i> (UNIX) • <i>kafka_bootstrap_servers</i> (UNIX) • <i>kafka_keytab</i> (UNIX) • <i>kafka_principal</i> (UNIX) • <i>kafka_reader_enabled</i> (UNIX) • <i>kafka_topic_name</i> (UNIX) • <i>kafka_use_tls</i> (UNIX) • <i>kerberos_plugin_dir</i> (UNIX) • <i>khash_max_entries</i> (UNIX) • <i>khash_table_length</i> (UNIX) • <i>krb_mssql_driver_installed</i> (Windows) • <i>krb_mssql_driver_nonblocking</i> (Windows) • <i>krb_mssql_driver_on-demand</i> (Windows) • <i>krb_mssql_driver_user_collect_time</i> (UNIX, Windows) • <i>ktap_buffer_flush</i> (UNIX) • <i>ktap_buffer_size</i> (UNIX) • <i>ktap_dbgev_ev_list</i> (UNIX) • <i>ktap_dbgev_func_name</i> (UNIX) • <i>ktap_fast_file_verdict</i> (UNIX) • <i>ktap_fast_tcp_verdict</i> (UNIX) • <i>ktap_installed</i> (UNIX) • <i>ktap_request_timeout</i> (UNIX) • <i>lhmon_driver_installed</i> (Windows) • <i>lhmon_for_network</i> (Windows) • <i>load_balancer_ip</i> (UNIX, Windows) • <i>load_balancer_load_affinity</i> (UNIX) • <i>load_balancer_num_mus</i> (UNIX, Windows) • <i>log4j_listen_address</i> (UNIX) • <i>log4j_num_connections</i> (UNIX) • <i>log4j_port</i> (UNIX, Windows) • <i>log4j_reader_enabled</i> (UNIX) • <i>log_program_name</i> (UNIX) • <i>max_server_write_size</i> (UNIX) • <i>min_bytes_to_compress</i> (UNIX, Windows) • <i>modification_count</i> (UNIX, Windows) • <i>modification_host</i> (UNIX, Windows) • <i>modification_microsec</i> (UNIX, Windows) • <i>msg_aggregate_timeout</i> (UNIX) • <i>msg_count_watermark</i> (UNIX) • <i>named_pipes_driver_installed</i> (Windows) • <i>network_namedpipes</i> (Windows) • <i>number_of_processors</i> (Windows) • <i>ora_driver_installed</i> (Windows) • <i>participate_in_load_balancing</i> (UNIX, Windows,i) • <i>pcap_backup_ktap</i> (UNIX, Windows) • <i>pcap_buffer_size</i> (UNIX) • <i>pcap_dispatch_count</i> (UNIX) • <i>pcap_read_timeout</i> (UNIX) • <i>private_tap_ip</i> (UNIX) • <i>qrw_default_state</i> (UNIX) • <i>qrw_force_unwatch</i> (UNIX) • <i>qrw_force_watch</i> (UNIX) • <i>qrw_installed</i> (UNIX) • <i>remote_messages</i> (UNIX, Windows,i) • <i>shared_memory_driver_installed</i> (Windows) • <i>sqlguard_cert_cn</i> (UNIX) • <i>stap_statistic</i> (UNIX) • <i>stap_statistic_version</i> (UNIX, Windows) • <i>sybase_driver_installed</i> (Windows) • <i>syslog_messages</i> (UNIX, Windows) • <i>tap_buf_dir</i> (UNIX) • <i>tap_debug_output_level</i> (UNIX) • <i>tap_failover_session_quiesce</i> (UNIX) • <i>tap_failover_session_size</i> (UNIX) • <i>tap_identifier</i> (UNIX, Windows) • <i>tap_ip</i> (UNIX, Windows) • <i>tap_log_dir</i> (UNIX) |

| Parameter | Value type | Description |
|-----------------|------------|---|
| | | <ul style="list-style-type: none"> • <i>tap_run_as_root</i> (UNIX) • <i>tee_installed</i> (UNIX) • <i>tee_msg_buf_len</i> (UNIX) • <i>tracefiles_dir</i> (Windows) • <i>uid_chain_sshd_ip</i> (UNIX) • <i>upload_feature</i> (UNIX, Windows) • <i>use_tls</i> (UNIX, Windows,i) • <i>wait_for_db_exec</i> (UNIX) <p>DB section:</p> <ul style="list-style-type: none"> • <i>connect_to_ip</i> (UNIX) • <i>db2_client_offset</i> (UNIX, Windows) • <i>db2_fix_pack_adjustment</i> (UNIX, Windows) • <i>db_exec_file</i> (UNIX) • <i>db_install_dir</i> (UNIX) • <i>db_user</i> (UNIX) • <i>db_version</i> (UNIX, Windows) • <i>encryption</i> (UNIX) • <i>exclude_networks</i> (UNIX, Windows) • <i>instance_name</i> (Windows) • <i>intercept_types</i> (UNIX) • <i>named_pipe</i> (Windows) • <i>networks</i> (UNIX, Windows) • <i>port_range_end</i> (UNIX, Windows) • <i>port_range_start</i> (UNIX, Windows) • <i>priority_count</i> (UNIX, Windows) • <i>real_db_port</i> (UNIX, Windows) • <i>tap_db_process_names</i> (Windows) • <i>unix_domain_socket_marker</i> (UNIX) <p>SQLGUARD section:</p> <ul style="list-style-type: none"> • <i>connection_pool_size</i> (UNIX) • <i>num_main_thread</i> (UNIX) • <i>sqlguard_ip</i> (UNIX, Windows, i) <p>SQLC_n section (UNIX Oracle Unified Auditing only):</p> <ul style="list-style-type: none"> • <i>data_pull_interval</i> (UNIX) • <i>instance</i> (UNIX) • <i>username</i> (UNIX) • <i>roles</i> (UNIX) • <i>data_pull_num_rows</i> (UNIX) |
| waitForResponse | String | <p>Specifies whether the API waits for a response from the S-TAP. Valid values:</p> <ul style="list-style-type: none"> • 0: do not wait • 1: wait for a response <p>The default is 1 when <i>stapHost</i> is a single host name or IP address, and 0 in all other cases.</p> |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • <i>all_managed</i>: execute on all managed units but not the central manager • <i>all</i>: execute on all managed units and the central manager • <i>group:<group name></i>: execute on all managed units identified by <i><group name></i> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <i>api_target_host=10.0.1.123</i>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <i>api_target_host=10.0.1.123</i>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

For all active UNIX S-TAPs: in the [TAP] section, set *all_can_control* to 1; set *qrw_default_state* to 0; in the [SQLGUARD] section, set *num_main_thread* to 4:

```
> grdapic update_stap_config stapHost=all_unix_active
updateValue=tap.all_can_control:1&tap.qrw_default_state:0&sqlguard.num_main_thread:4
```

or

```
> grdapic update_stap_config stapHost=all_unix_active updateValue=tap.all_can_control:1
update_stap_config stapHost=all_unix_active updateValue=tap.qrw_default_state:0
update_stap_config stapHost=all_unix_active updateValue=sqlguard.num_main_thread:4
```

For Windows, use this GRDAPIC to turn on the firewall. For example:

```
> grdapic update_stap_config stapHost=MyHost updateValue=TAP.FIREWALL_INSTALLED:1 waitForResponse=1
ID=77039
```

Related concepts

- [Editing the Linux-UNIX S-TAP configuration parameters](#)
- [Editing the Windows S-TAP configuration parameters](#)

Related reference

- [S-TAP and inspection engine APIs](#)

update_test_detail_exception

This command updates test detail exceptions.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/test_detail_exception
```

GuardAPI syntax

```
update_test_detail_exception parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------------------|------------|--|
| assessmentDesc | String | |
| assessmentScope | String | |
| datasourceGroup | String | |
| datasourceName | String | |
| datasourceScope | String | |
| datasourceType | String | |
| detailExceptionValue | String | |
| exceptionType | String | Valid values: <ul style="list-style-type: none">• <code>text</code>• <code>regex</code>• <code>0</code>• <code>1</code> |
| explanation | String | |
| fromDate | String | |
| testDescription | String | |
| testDetailExceptionsId | String | Required. |
| toDate | String | |

update_test_exception

This command updates test exceptions.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/test_exception
```

GuardAPI syntax

```
update_test_exception parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|--|
| assessmentDesc | String | |
| assessmentScope | String | Valid values: <ul style="list-style-type: none">• CURRENT• ALL• 0• 1 |
| datasourceGroup | String | |
| datasourceName | String | |
| datasourceScope | String | Valid values: <ul style="list-style-type: none">• SINGLE• GROUP• ALL• 0• 1• 2 |
| datasourceType | String | For valid values, call update_test_exception from the command line with --help=true. |
| explanation | String | |
| fromDate | String | |
| testDescription | String | |
| testExceptionId | Long | Required. |
| toDate | String | |

update_threshold_in_rule

Use this API to change the threshold on a specific violation policy rule that is used to create an active threat analytics case type.

Changes to installed policies are applied according to the policy schedule. When adding a threshold to a rule in an installed policy, cases are created for violations (according to the threshold) only after the policy is reinstalled.

This API is available in Guardium V11.2 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/update_threshold_in_rule
```

GuardAPI syntax

```
update_threshold_in_rule parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| policy_name | String | The policy that has the rule whose threshold you want to change. Use the API list_policy to view policies. |
| rule_name | String | The rule whose threshold you want to change. Use the API list_policy_rules to view rules. |
| threshold_value | Integer | The threshold at which a case is created. |

Examples

To change the threshold to 50 in the ruleNNN in policyAAA:

```
grdapic update_threshold_in_rule policy_name=policyAAA rule_name=ruleNNN threshold=50
```

Related tasks

- [Creating threat categories from policy rules](#)

Related reference

- [add_threshold_to_rule](#)
- [list_policy_rules](#)
- [list_policy](#)
- [remove_threshold_from_rule](#)

update_user

Update information for a Guardium user.

To make changes to roles for this user, use the [set_user_roles](#) API.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/user
```

GuardAPI syntax

```
update_user parameter=value
```

Parameters

| Parameter | Value type | Description |
|-------------------|------------|--|
| confirmPassword | String | Required. Confirm the password. The confirmPassword must match the value of Password. |
| country | String | The ISO 3166 2-letter country code for this user, such as US or ES. For valid values, call update_user from the command line with --help=true . |
| disabled | Boolean | Enables or disables this user. Valid values: <ul style="list-style-type: none">• 0 (false): The user is enabled.• 1 (true): The user is disabled. Default = 0 |
| disablePwdExpiry | Boolean | Valid values: <ul style="list-style-type: none">• 0 (false)• 1 (true) Default = 1 (true) |
| email | String | The user's email address |
| firstName | String | The user's given name. |
| lastName | String | The user's family name. |
| password | String | Required. The password must be at least 8 characters long and include at least one of each: <ul style="list-style-type: none">• An uppercase letter (A-Z)• A lowercase letter (a-z)• A number (0-9)• A special character, which can be: at sign (@), hashtag (#), dollar sign (\$), percent sign (%), caret (^), ampersand (&), asterisk (*), exclamation (!), hyphen (-), underscore (_), plus (+), or equals (=). |
| smartCardUserName | String | Common name in the certificate.
Enter the smart card user name when smart card authentication is turned on. |
| userName | String | Required. A user name for this user.
The following characters are not allowed in user names: semicolon (;), forward slash (/), dollar sign (\$), and percent sign (%). |

Examples

After using the [create_user](#) API to create a new user named Fred McDerf, you realize that you forgot to add his email address. Use [update_user](#) to add the email address as follows:

```
grdapi update_user userName="Fred McDerf" email=fredmcd@company.com
```

Related concepts

- [User account, password, and authentication CLI Commands](#)

Related reference

- [create_user](#)
- [list_roles](#)
- [set_user_roles](#)

update_user_db

This command applies all recent changes to the active User-DB association map.

After you run some commands, you also need to run [update_user_db](#) to apply the changes.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the **PUT** method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/user_db
```

GuardAPI syntax

```
update_user_db parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">all_managed: execute on all managed units but not the central managerall: execute on all managed units and the central managergroup:<group name>: execute on all managed units identified by <group name>host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

After you run some commands, such as `create_allowed_db`, you must run `update_user_db`.

```
grdapi create_allowed_db userName=Fred serverIp=192.168.1.1 instanceName=test
```

Sample output

```
ID=1
When complete, in order for synchronization to take effect, run update_user_db
ok

grdapi update_user_db
ID=0
A background process updates the database. The results are not immediate.
ok
```

Related concepts

- [Data Security - User Hierarchy and Database Associations](#)

Related reference

- [create_allowed_db](#)

update_utilization_thresholds

This API is available in Guardium V9.5 and later.

GuardAPI syntax

```
update_utilization_thresholds parameter=value
```

Parameters

| Parameter | Value type | Description |
|------------|------------|---|
| paramName | String | Required. For valid values, call <code>update_utilization_thresholds</code> from the command line with <code>--help=true</code> . |
| threshold1 | Integer | Required. |
| threshold2 | Integer | Required. |

upload_custom_data

This command uploads data to a pre-configured custom table.

Before you run this command, you need to configure a custom table from the Custom Table Builder in the GUI (Reports > Report Configuration Tools > Custom Table Builder). Select a Custom Table, click Upload Data, and add or select a datasource.

This API is available in Guardium V9.5 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/custom_data
```

GuardAPI syntax

```
upload_custom_data parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| tableName | String | Required. The name of the custom table to which to upload data. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none">• <code>all_managed</code>: execute on all managed units but not the central manager• <code>all</code>: execute on all managed units and the central manager• <code>group:<group name></code>: execute on all managed units identified by <code><group name></code>• host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>.• host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

GuardAPI example

```
grdapi upload_custom_data tableName="MY_TABLE"
```

Related concepts

- [External Data Correlation](#)

venafi_import

Use this command to import a Venafi certificate.

This API is available in Guardium v11.3 and later.

REST API syntax

This API is available as a REST service with the `PUT` method. Call this API as follows:

```
PUT https://[Guardium hostname or IP address]:8443/restAPI/venafi_import
```

GuardAPI syntax

```
venafi_import parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|--|
| variant | String | Required. Valid values: <ul style="list-style-type: none">• <code>sniffer</code>• <code>gui</code>• <code>gim</code> |

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Example

```
grdapi venafi_import variant=gui force=true api_target_host=all
```

Related tasks

- [Managing certificates by using Venafi](#)

verify_cyberark_access

This command tests the connection to the CyberArk server.

This API is available in Guardium V11.0 and later.

REST API syntax

This API is available as a REST service with the `GET` method. Call this API as follows:

```
GET https://[Guardium hostname or IP address]:8443/restAPI/cyberark
```

GuardAPI syntax

```
verify_cyberark_access parameter=value
```

Parameters

| Parameter | Value type | Description |
|--------------------|------------|-------------|
| vaultPassword | String | Required. |
| vaultUserName | String | Required. |
| vaultWebServerName | String | Required. |

Example

```
grdapi verify_cyberark_access vaultUserName=username vaultPassword=passwprd vaultWebServerName=servername.com
```

verify_stap_inspection_engine_with_sequence

Use this command to perform verification of the specified S-TAP® inspection engine..

This GuardAPI is available in Guardium V9.5 and later.

The REST API is available in V11.1 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/verify_stap_inspection_engine_with_sequence
```

GuardAPI syntax

```
verify_stap_inspection_engine_with_sequence parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------------|------------|---|
| addToSchedule | String | Whether or not to add this inspection engine to the scheduled verification. Valid values: <ul style="list-style-type: none">• Yes• No |
| datasourceName | String | If this parameter is specified, advanced verification is performed against the specified datasource. If this parameter is omitted, standard verification is performed. |
| protocol | String | Required. The database protocol. |
| sequence | Integer | The sequence number of the inspection engine to be removed within the set of inspection engines of the specified type. Use the <code>grdapi list_inspection_engines</code> command with the type option first to verify the sequence number. |
| stapHost | String | Required. The host name or IP address of the database server on which the S-TAP is installed. |
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • <code>all_managed</code>: execute on all managed units but not the central manager • <code>all</code>: execute on all managed units and the central manager • <code>group:<group name></code>: execute on all managed units identified by <code><group name></code> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Examples

To initiate standard verification of the S-TAP with the sequence number of 4, on an MYSQL database, with the IP address 12.12.12.12:

```
grdapi verify_stap_inspection_engine_with_sequence stapHost=12.12.12.12 protocol=mysql sequence=4
```

Related concepts

- [Inspection engine configuration](#)

Related tasks

- [Linux-UNIX: Configuring an inspection engine](#)
- [Windows: Configuring an inspection engine](#)

Related reference

- [S-TAP and inspection engine APIs](#)

wkc_refresh_external_pwd

If you use an external configuration manager to connect to IBM® Knowledge Catalog, this API updates the configuration manager password.

For more information, see [Starting the IBM Knowledge Catalog and Guardium Data Protection integration](#).

This API is available in Guardium v12.0 and later.

REST API syntax

This API is available as a REST service with the `POST` method. Call this API as follows:

```
POST https://[Guardium hostname or IP address]:8443/restAPI/wkc_refresh_external_pwd
```

GuardAPI syntax

```
wkc_refresh_external_pwd parameter=value
```

Parameters

| Parameter | Value type | Description |
|-----------|------------|-------------|
|-----------|------------|-------------|

| Parameter | Value type | Description |
|-----------------|------------|---|
| api_target_host | String | <p>Specifies the target hosts where the API executes. Valid values:</p> <ul style="list-style-type: none"> • all_managed: execute on all managed units but not the central manager • all: execute on all managed units and the central manager • group:<group name>: execute on all managed units identified by <group name> • host name or IP address of a managed unit: specified from the central manager to execute on a managed unit. For example, <code>api_target_host=10.0.1.123</code>. • host name or IP address of the central manager: specified from a managed unit to execute on the central manager. For example, <code>api_target_host=10.0.1.123</code>. <p>IP addresses must conform to the IP mode of your network. For dual IP mode, use the same IP protocol with which the managed unit is registered with the central manager. For example, if the registration uses IPv6, specify an IPv6 address. The hostname is independent of IP mode and can be used with any mode.</p> |

Access management APIs

Use these commands to manage access to the Guardium system. Many of these commands require the accessmgr role.

CLI password APIs

Use the following APIs to manage CLI passwords:

- [change_cli_password](#)
- [enable_strong_cli_password](#)

Custom LDAP table APIs

- [create_custom_table_ldap_import](#)
- [delete_custom_table_ldap_import](#)
- [list_custom_table_ldap_imports](#)
- [run_custom_table_ldap_import](#)
- [update_custom_table_ldap_import](#)

Multi-factor authentication APIs

The following APIs help manage multi-factor (two-factor) authentication. For more information, see [Multi-factor \(two-factor\) authentication](#).

- [add_mfa_exempt_users](#)
- [configure_mfa](#)
- [get_mfa_configuration](#)
- [remove_mfa_exempt_users](#)

Oauth APIs

The following APIs manage OAuth functions.

- [delete_oauth_clients](#)
- [getOAuthTokenExpirationTime](#)
- [list_oauth_clients](#)
- [modify_oauth_validity](#)
- [register_oauth_client](#)
- [register_oauth_internal_client](#)
- [revokeOAuthClient](#)
- [revokeOAuthToken](#)
- [setOAuthTokenExpirationTime](#)

Role and user APIs

The following APIs manage users, roles, and role relationships. For more information about setting roles, see [Security Roles](#).

Note: In a central management environment, the object to which you want to add a role might reside on either the central manager or on a managed unit.

- [create_role](#)
- [create_user](#)
- [delete_user](#)
- [grant_role_to_object_by_id](#)
- [grant_role_to_object_by_Name](#)
- [list_roles](#)
- [list_roles_granted_to_object_by_id](#)
- [list_roles_granted_to_object_by_Name](#)
- [list_users](#)
- [list_user_roles](#)
- [retrieveUpdatedUsers](#)

- [revoke_role_from_object_by_id](#)
- [revoke_role_from_object_by_Name](#)
- [set_user_roles](#)
- [update_user](#)

User hierarchy APIs

The following APIs manage user hierarchy relationships. For more information, see [Data Security - User Hierarchy and Database Associations](#).

- [create_user_hierarchy](#)
- [delete_user_hierarchy_by_entry_id](#)
- [delete_user_hierarchy_by_user](#)
- [list_user_hierarchy_by_parent_user](#)

User-DB association APIs

The following APIs manage user-database associations. For more information, see [Data Security - User Hierarchy and Database Associations](#).

- [create_allowed_db](#)
- [delete_allowed_db_by_entry_id](#)
- [delete_allowed_db_by_user](#)
- [list_allowed_db_by_user](#)
- [update_user_db](#)

Active threat analytics and risk spotter APIs

Use these commands to configure Active threat analytics and Risk spotter.

Active threat analytics:

- [add_threshold_to_rule](#)
- [disable_threat_finder](#)
- [enable_threat_finder](#)
- [list_rules_with_threshold](#)
- [remove_threshold_from_rule](#)
- [update_threshold_in_rule](#)

Risk spotter:

- [disable_riskspotter](#)
- [enable_riskspotter](#)
- [riskspotter_set_config](#)

Related concepts

- [Active threat analytics](#)
- [Risk spotter](#)
- [Risk spotter risk indicators](#)

Related tasks

- [Creating threat categories from policy rules](#)

Alerter APIs

Use these APIs to manage alerter functions.

- [delete_alerter_snmp_settings](#)
- [set_alerter_settings](#)
- [set_alerter_smtp_settings](#)
- [set_alerter_snmp_settings](#)
- [show_alerter_settings](#)
- [show_alerter_smtp_settings](#)
- [show_alerter_snmp_settings](#)
- [show_alerter_status](#)
- [stop_restart_alerter](#)

Archive, export, import, purge, and restore APIs

Use these functions to configure archive, restore, purge, export, and import, of results and data.

- [configure_archive](#)
- [configure_export](#)
- [configure_purge](#)
- [configure_results_archive](#)
- [configure_results_export](#)
- [delete_archive_configuration](#)
- [delete_export_configuration](#)
- [delete_results_archive_configuration](#)
- [delete_results_export_configuration](#)
- [disable_purge](#)
- [export_definition](#)
- [export_transfer_key](#)
- [generate_transfer_key](#)
- [get_expiration_date_for_restored_day](#)
- [get_purge_batch_size](#)
- [import_definitions](#) (REST API only)
- [list_compatibility_modes](#)
- [list_ready_files](#)
- [rest_export_definition](#)
- [set_expiration_date_for_restored_day](#)
- [set_import](#)
- [set_purge_batch_size](#)

Related concepts

- [Managing data: archive, restore, aggregation, and system backup](#)

Related reference

- [Catalog entry APIs](#)
-

Assessment APIs

Use these APIs to add, delete, and update Vulnerability Assessment (VA) functions.

Assessment APIs

- [add_assessment_datasource](#)
- [add_assessment_datasource_group](#)
- [add_assessment_test](#)
- [add_assessment_test_by_dsid](#)
- [add_available_test_notes](#)
- [clone_assessment](#)
- [create_ad_hoc_audit_for_security_assessment](#)
- [create_assessment](#)
- [delete_assessment](#)
- [delete_assessment_datasource](#)
- [delete_assessment_datasource_group](#)
- [delete_assessment_test](#)
- [delete_available_test_notes](#)
- [execute_assessment](#)
- [get_assessment_result](#)
- [get_inapplicable_test_result_status](#)
- [list_assessments](#)
- [list_assessment_tests](#)
- [list_available_test_notes](#)
- [list_available_tests](#)
- [set_inapplicable_test_result_status](#)
- [update_assessment](#)
- [update_assessment_test](#)

Test exception APIs

- [create_test_detail_exception](#)
- [create_test_exception](#)
- [delete_test_detail_exception](#)
- [delete_test_detail_exception_by_id](#)
- [delete_test_exception](#)
- [delete_test_exception_by_id](#)
- [list_test_detail_exception](#)
- [list_test_exception](#)
- [list_test_exception_by_id](#)
- [update_test_detail_exception](#)
- [update_test_exception](#)

VA summary key APIs

- [get_va_summary_key](#)
 - [modify_va_summary_key](#)
 - [reset_va_summary_by_id](#)
 - [reset_va_summary_by_key](#)
-

Auto-discovery APIs

Use these GrdAPI commands to create, modify, list and run the Auto-discovery processes.

- [add_autodetect_task](#)
- [create_autodetect_process](#)
- [delete_autodetect_process](#)
- [delete_autodetect_scans_for_process](#)
- [execute_autodetect_process](#)
- [list_autodetect_processes](#)
- [list_autodetect_tasks_for_process](#)
- [modify_autodetect_process](#)
- [show_autodetect_process_status](#)
- [stop_autodetect_process](#)

Related concepts

- [Database auto-discovery](#)
-

Big Data Intelligence APIs

Run these commands, on your central manager, to manage extraction of datamarts to the Big Data datasource (GBDI), and to pull big data into Guardium for monitoring, reports, and so on.

Big Data Intelligence functions are:

- [add_dm_to_profile](#)
- [clone_extraction_profile](#)
- [disable_big_data_interface](#)
- [enable_big_data_interface](#)
- [get_extraction_profile_info](#)
- [local_disable_big_data_intelligence](#)
- [local_enable_big_data_interface](#)
- [remove_dm_from_profile](#)
- [remove_extraction_profile](#)
- [replace_active_profile](#)

Catalog entry APIs

Use these commands to manage catalog entries. Catalogs are used to track data archive files and result archive files that were created on the servers.

The catalog entry functions are:

- [create_entry_location](#)
 - [delete_entry_location](#)
 - [list_entry_location](#)
 - [update_entry_location](#)
-

Central management APIs

Use these APIs to view and set load balancing parameters, view the current load map, manage S-TAP® and managed unit group associations, and manage backup central managers.

Load balancing APIs

- [assign_load_balancer_groups](#)
- [get_load_balancer_load_map](#)
- [get_load_balancer_params](#)
- [set_load_balancer_param](#)
- [unassign_load_balancer_groups](#)

Other APIs

- [get_unit_data](#)
- [get_unit_pinger](#)
- [update_managed_units_ping_time](#)

Central manager APIs

- [backup_cm_list_candidates](#)
- [backup_cm_set](#)
- [list_managed_units](#)
- [make_primary_cm](#)
- [restart_all_managed_units](#)
- [restore_units_after_bad_shift](#)
- [set_certificate_host_validation](#)
- [show_backup_cm_ip](#)

Classification APIs

Use the following GuardAPI commands for Classification policy configuration, for test automation and, for scripting of prerequisite data preparation.

Note: Some discovery and classification settings are configured using the [modify_guard_param](#) command. For more information, see [modify_guard_param](#).

- [add_classifier_datasource](#)
- [add_classifier_datasource_group](#)
- [create_classifier_action](#)
- [create_classifier_policy](#)
- [create_classifier_process](#)
- [create_classifier_rule](#)
- [delete_classifier_action](#)
- [delete_classifier_policy](#)
- [delete_classifier_process](#)
- [delete_classifier_rule](#)
- [execute_cls_process](#)
- [get_job_process_concurrency_limit](#)
- [list_classifier_policy](#)
- [list_classifier_process](#)
- [set_job_process_concurrency_limit](#)
- [remove_classifier_datasource](#)
- [remove_classifier_datasource_group](#)
- [update_classifier_action](#)
- [update_classifier_log_level](#)
- [update_classifier_policy](#)
- [update_classifier_process](#)
- [update_classifier_rule](#)

Cloud datasource APIs

Use these commands to define, manage, update, and delete cloud datasources.

The cloud datasource APIs are

- [add_stream](#)
- [assign_collectors](#)
- [configure_data_streaming](#)
- [create_cloudTitle](#)
- [create_cloud_datasource](#)
- [delete_stream](#)
- [disable_datastream](#)
- [discover_streams](#)
- [enable_datastream](#)
- [enable_disable_monitoring_streams](#)
- [get_streams](#)
- [list_cloud_datasource_by_name](#)
- [restart_cloud_instance](#)
- [update_cloud_datasource](#)

Configuration Auditing System (CAS) APIs

Use these commands to configure and manage Configuration Auditing System (CAS) hosts, templates, and template sets.

The CAS functions are:

- [clear cas template set](#)
- [clone cas template set](#)
- [create cas host instance](#)
- [create cas template](#)
- [create cas template set](#)
- [delete cas host](#)
- [delete cas host instance](#)
- [delete cas template](#)
- [delete cas template set](#)
- [list cas hosts](#)
- [list cas host instances](#)
- [list cas templates](#)
- [list cas template sets](#)
- [update cas host instance](#)
- [update cas template](#)

Related concepts

- [Configuration Auditing System \(CAS\)](#)

Data mart APIs

Use these commands to manage your data marts.

- [datamart_copy_file_bundle](#)
- [datamart_include_file_header](#)
- [datamart_refresh_metadata](#)
- [datamart_run_once_now](#)
- [datamart_set_active](#)
- [datamart_set_date_format](#)
- [datamart_set_inactive](#)
- [datamart_update_copy_file_info](#)
- [datamart_validate_copy_file_info](#)
- [get_datamart_info](#)
- [rerun_datamart](#)
- [unschedule_datamart](#)
- [update_datamart](#)
- [update_datamart_copy_file_threadpool_params](#)

Related concepts

- [Data mart](#)

Database user APIs

Use these commands to maintain database user mapping, non-credential scans and manage debug levels.

The database user commands are:

- [create_db_user_mapping](#)
- [delete_db_user_mapping](#)
- [get_debug_level](#)
- [list_db_user_mapping](#)
- [non_credential_scan](#)
- [set_debug_level](#)

Datasource APIs

Use these commands to create, list, delete, and update datasource and datasource references.

Datasource APIs

Note: Some datasource settings are configured using the modify_guard_param command. For more information, see [modify_guard_param](#).

- [add_connection_properties](#)
- [create_datasource](#)
- [delete_datasource_by_id](#)
- [delete_datasource_by_name](#)
- [delete_datasource_configuration](#)

- [list_datasource_by_id](#)
- [list_datasource_by_name](#)
- [list_db_drivers](#)
- [list_db_drivers_by_details](#)
- [remove_connection_properties](#)
- [remove_datasource_configuration_from_collector](#)
- [save_datasource_configuration_on_collector](#)
- [test_datasource_connection](#)
- [update_datasource_by_id](#)
- [update_datasource_by_name](#)

Datasource custom property APIs

- [add_custom_property_to_datasource_by_id](#)
- [add_custom_property_to_datasource_by_name](#)
- [add_custom_property_to_datasources_in_group](#)
- [create_datasource_custom_property](#)
- [delete_datasource_custom_property](#)
- [get_datasource_custom_properties](#)
- [remove_custom_property_from_datasource_by_id](#)
- [remove_custom_property_from_datasource_by_name](#)
- [remove_custom_property_from_datasources_in_group](#)
- [update_datasource_custom_property](#)

Datasource group APIs

- [add_datasource_to_group](#)
- [create_datasource_group](#)
- [create_datasource_groupRef_by_id](#)
- [create_datasource_groupRef_by_name](#)
- [delete_datasource_group](#)
- [delete_datasource_groupRef_by_id](#)
- [delete_datasource_groupRef_by_name](#)
- [list_datasource_group_hierarchy](#)
- [list_datasource_group_members](#)
- [list_datasource_groups](#)
- [list_datasource_groupRef_by_id](#)
- [list_datasource_groupRef_by_name](#)
- [remove_datasource_from_group](#)
- [update_datasource_credentials_in_group](#)
- [update_datasource_group](#)

Datasource reference APIs

- [create_datasourceRef_by_id](#)
- [create_datasourceRef_by_name](#)
- [delete_datasourceRef_by_id](#)
- [delete_datasourceRef_by_name](#)
- [list_datasourceRef_by_id](#)
- [list_datasourceRef_by_name](#)

Mongo DB datasource APIs

- [load_mongodb](#)
- [load_mongodb_by_datasource](#)

Datasource credential management APIs

Use these commands to manage datasource credentials.

AWS Secrets Manager APIs

- [create_aws_secrets_manager_config](#)
- [delete_aws_secrets_manager_config](#)
- [list_aws_secrets_manager_config](#)
- [update_aws_secrets_manager_config](#)

For more information about the AWS secrets manager, see [Managing datasource credentials with AWS Secrets Manager](#).

CyberArk APIs

- [create_cyberark_config](#)
- [delete_cyberark_config](#)

- [list_cyberark_config](#)
- [update_cyberark_config](#)
- [verify_cyberark_access](#)

For more information about CyberArk, see [Managing datasource credentials with CyberArk](#).

HashiCorp APIs

- [create_hashicorp_config](#)
- [delete_hashicorp_config](#)
- [list_hashicorp_config](#)
- [test_hashicorp_connection](#)
- [update_hashicorp_config](#)

For more information about HashiCorp, see [Managing datasource credentials with HashiCorp](#).

Entitlement optimization APIs

Use these API commands to enable and configure the Entitlement optimization datasources and reporting.

- [add_datasource_to_entitlement_optimization](#)
- [disable_entitlement_optimization](#)
- [enable_entitlement_optimization](#)
- [get_entitlement_optimization_info](#)
- [remove_datasource_from_entitlement_optimization](#)
- [set_entitlement_datasource_parameter](#)

Related concepts

- [Entitlement Optimization](#)
-

External feed APIs

Use these commands to create mappings for external feeds.

- [create_ef_mapping](#)
- [delete_ef_mapping](#)
- [list_ef_mapping](#)
- [list_ef_report](#)
- [modify_ef_mapping](#)
- [modify_ef_sql_mode](#)

File Activity Monitor APIs

Use the following GuardAPI commands to enable and disable the file activity monitor, configure the file Investigation Dashboard activity and entitlement extractions schedule, and get information on the file activity monitor.

The File Activity Monitoring functions are:

- [add_action_to_fam_rule](#)
- [create_fam_rule](#)
- [create_policy](#)
- [delete_policy](#)
- [disable_fam_crawler](#)
- [enable_fam_crawler](#)
- [get_fam_crawler_info](#)
- [list_policy_fam_rule](#)
- [policy_fam_rule_delete](#)

Related concepts

- [Discovery and classification in Windows and Unix-Linux file servers](#)
 - [File Activities policies and rules](#)
-

Guardium Insights APIs

Use these APIs to manage the connection between Guardium® Data Protection and Guardium Insights.

- [get_insights_agent_config](#)

- [insights_registration](#)
 - [insights_unregistration](#)
 - [push_insights_trust](#)
 - [migrate_stap_config](#)
 - [update_insights_agent_config](#)
 - [update_insights_registration_config](#)
-

Guardium Installation Manager (GIM) APIs

Use these APIs to assign, cancel, list, remove, and update Guardium Installation Manager (GIM) functions.

The GIM API commands are:

- [gim_assign_bundle_or_module_to_client_by_version](#)
 - [gim_assign_latest_bundle_or_module_to_client](#)
 - [gim_cancel_install](#)
 - [gim_cancel_uninstall](#)
 - [gim_get_available_modules](#)
 - [gim_get_client_last_event](#)
 - [gim_get_global_param](#)
 - [gim_get_modules_running_status](#)
 - [gim_list_bundles](#)
 - [gim_list_client_modules](#)
 - [gim_list_client_params](#)
 - [gim_list_mandatory_params](#)
 - [gim_list_registered_clients](#)
 - [gim_list_unused_bundles](#)
 - [gim_load_package](#)
 - [gim_remote_activation](#)
 - [gim_remove_bundle](#)
 - [gim_reset_client](#)
 - [gim_schedule_install](#)
 - [gim_schedule_uninstall](#)
 - [gim_set_diagnostics](#)
 - [gim_set_global_param](#)
 - [gim_unassign_client_module](#)
 - [gim_uninstall_module](#)
 - [gim_update_client_params](#)
 - [run_diagnostics](#)
-

Guardium universal connector APIs

Use these functions to start, stop, and check the status of the Guardium universal connector, and to modify the MongoDB filters.

- [add_domain_to_universal_connector_allowed_domains](#)
- [backup_universal_connector](#)
- [disable_persistent_queue_universal_connector](#)
- [enable_persistent_queue_universal_connector](#)
- [generate_ssl_key_universal_connector](#)
- [get_universal_connector_allowed_domains](#)
- [get_universal_connector_status](#)
- [reboot_image_universal_connector](#)
- [restore_universal_connector](#)
- [remove_domain_from_universal_connector_allowed_domains](#)
- [run_universal_connector](#)
- [schedule_generate_mongo_filter_job](#)
- [set_universal_connector_log_level](#)
- [show_universal_connector_plugins](#)
- [stop_universal_connector](#)
- [universal_connector_disable_metrics](#)
- [universal_connector_enable_metrics](#)
- [universal_connector_keystore_add](#)
- [universal_connector_keystore_list](#)
- [universal_connector_keystore_remove](#)
- [universal_connector_update_proxy](#)

Related concepts

- [Guardium universal connector](#)
-

Group APIs

Use these commands to create, list, and delete groups, hierarchical groups, and group members and manage aliases for groups.

Note: In a central management environment, all groups are defined on the central manager and sent to the managed units on a scheduled basis.

- [create_alias](#)
- [create_group](#)
- [create_hierarchical_member_to_group_by_desc](#)
- [create_member_to_group_by_desc](#)
- [create_member_to_group_by_id](#)
- [create_member_to_group_DAMX_Standard_Activity](#)
- [create_member_to_group_DAMX_Suspicious_Connections](#)
- [delete_alias](#)
- [delete_group_by_desc](#)
- [delete_group_by_id](#)
- [delete_hierarchical_member_from_group_by_desc](#)
- [delete_member_from_group_by_desc](#)
- [delete_member_from_group_by_id](#)
- [flatten_hierarchical_groups](#)
- [list_aliases](#)
- [list_group_by_desc](#)
- [list_group_by_id](#)
- [list_group_members_by_desc](#)
- [list_group_members_by_id](#)
- [list_groups](#)
- [populate_group_from_query](#)
- [populateMembersForGroup](#)
- [remove_populate_group_from_query](#)
- [run_populate_group_from_query](#)
- [set_populate_group_from_query_schedule](#)
- [update_alias](#)
- [update_group_by_desc](#)
- [update_group_by_id](#)

Related concepts

- [Groups](#)

Health analyzer APIs

Use these commands to configure the disk and database health analyzer.

Note: Some disk and database health analyzer settings are configured using the `modify_guard_param` command. For more information, see [modify_guard_param](#).

- [disable_health_analyzer](#)
- [enable_health_analyzer](#)
- [enable_health_traffic_job](#)
- [get_health_traffic_status](#)
- [set_health_traffic_job_interval](#)

Hadoop monitoring APIs

Use these APIs to add, update, delete, and view the clusters and services on the clusters for all types monitoring on Hadoop.

Hadoop integration using Ranger HDFS for Hortonworks and Cloudera 7

The commands for Cloudera 7 HDFS configuration are:

- [add_ranger_hdfs_config](#)
- [delete_ranger_hdfs_config](#)
- [get_ranger_hdfs_config](#)
- [update_ranger_hdfs_config](#)

Hadoop integration using Hortonworks and Apache Ranger Log4J

The commands for Apache Ranger configuration are:

- [add_ranger_config](#)
- [add_ranger_service](#)
- [disable_monitoring_ranger_service](#)
- [enable_monitoring_ranger_service](#)
- [get.hadoop_cluster_status](#)
- [get_ranger_config](#)
- [get_ranger_services_status](#)
- [list_ranger_configs](#)

- [list_ranger_staps](#)
- [remove_ranger_config](#)
- [remove_ranger_service](#)
- [update_ranger_config](#)
- [update_ranger_service](#)

Related concepts

- [Hadoop integration using Ranger HDFS for Hortonworks and Cloudera 7](#)
- [Hadoop integration using Hortonworks and Apache Ranger Log4J](#)

Related reference

- [S-TAP Hadoop parameters](#)

Investigation dashboard APIs

Use these APIs to enable, disable, or configure the investigation dashboard (quick search) features and parameters.

The investigation dashboard includes the Quick Search Results Table, in addition to the Activity Chart, and various other pre-defined charts.

- [add_group_to_quick_search](#)
- [delete_group_from_quick_search](#)
- [disable_quick_search](#)
- [enable_quick_search](#)
- [get_quick_search_info](#)
- [list_quick_search_groups](#)
- [quick_search](#) (REST API only)
- [refresh_quick_search_groups](#)
- [set_enterprise_search_options](#)

Related concepts

- [Investigation dashboard](#)

Miscellaneous APIs

Use these commands for various tasks that do not fall into other categories.

Other miscellaneous APIs

- [change_to_opensource](#)
- [export_certificate](#)
- [export_config](#)
- [encrypt_value](#)
- [nscd](#)
- [pause_or_resume_scenarios](#)
- [venafi_import](#)
- [wkc refresh_external_pwd](#)

Change tracker APIs

- [change_tracker_get_events](#)
- [change_tracker_get_params](#)
- [change_tracker_get_tasks](#)
- [change_tracker_reset](#)
- [change_tracker_set_params](#)

Custom table distribution APIs

- [delete_cust_table_distribution_schedule](#)
- [sched_cust_table_distribution](#)

Discovered instances APIs

- [apply_rules_on_discoveredinstances](#)
- [run_database_instance_discovery](#)

Eastern font APIs

- [disable_embed_eastern_font](#)
- [enable_embed_eastern_font](#)

F5 integration APIs

- [f5_add_apps_config](#)
- [f5_add_data_params](#)
- [f5_delete_apps_config](#)
- [f5_delete_data_params](#)
- [f5_list_apps_config](#)
- [f5_list_data_params](#)
- [f5_update_data_params](#)

FIPS mode APIs

- [clevus_bind](#)
- [enable_fips_tls](#)
- [fipsmode](#)

IP Aliasing APIs

- [disable_ip_to_host_aliases](#)
- [enable_ip_to_host_aliases](#)
- [get_ip_to_alias_overwrites](#)
- [get_ip_to_alias_selected](#)
- [set_ip_to_alias_overwrites](#)
- [set_ip_to_alias_selected](#)

Keystore APIs

- [copy_key_file](#)
- [pull_external_stap_keystore](#)

Modifiable guard_param APIs

- [get_all_modifiable_guard_params](#)
- [get_guard_param](#)
- [modify_guard_param](#)
- [push_parameter_to_mu](#)

Patch APIs

- [patch_cleanup](#)
- [patch_install](#)

REST APIs

The following APIs are only available as REST APIs and are generally used to find and manage other REST APIs.

- [create_online_report](#)
- [get_definitions_data_sets](#)
- [get_definitions_items](#)
- [import_definitions](#)
- [rest_export_definition](#)
- [retrieveAPIs](#)
- [retrieveApiParameters](#)

Session inference APIs

- [session_inference_control](#)
- [session_inference_setup](#)

TLS protocol APIs

- [enable_all_tls](#)
- [enable_fips_tls](#)
- [enable_latest_tls](#)
- [get_secured_protocols_info](#)

Unit pinger APIs

- [get_unit_pinger](#)
- [restart_unit_pinger](#)

Unit utilization APIs

- [list_utilization_thresholds](#)
- [reset_unit_utilization_data](#)
- [update_utilization_thresholds](#)

z/OS IMS checkpoint APIs

- [delete_imscheckpoint_record](#)
- [list_imscheckpoint_records](#)

Native audit APIs

Use these commands to enable or disable DB Audit (native audit) on a cloud database, add and remove objects from the Object Audit (audit trail), and get configuration, collectors, and objects details.

The Native Audit functions are:

- [add_ip_to_sg](#)
- [add_objects_native_audit](#)
- [disable_native_audit](#)
- [enable_native_audit](#)
- [get_native_audit_collectors](#)
- [get_native_audit_configurations](#)
- [get_native_audit_objects](#)
- [remove_objects_native_audit](#)

Related tasks

- [Cloud database service protection with native audit](#)

Outliers detection APIs

Use these API commands to enable, disable, and configure the Outliers Detection function.

- [disable_outliers_detection](#)
- [disable_outliers_detection_agg](#)
- [disable_outliers_detection_cross_cm_agg](#)
- [disable_outliers_detection_cross_cm_collector](#)
- [enable_outliers_detection](#)
- [enable_outliers_detection_agg](#)
- [enable_outliers_detection_cross_cm_agg](#)
- [enable_outliers_detection_cross_cm_collector](#)
- [get_outliers_detection_info](#)
- [reregister_agg_collector](#)
- [set_outliers_detection_demo_mode](#)
- [set_outliers_detection_parameter](#)
- [set_outliers_detection_to_factory_settings](#)
- [set_outliers_user_detection_mode](#)
- [switch_outliers_user_mode](#)

Related concepts

- [Outliers detection](#)

Policy and rule APIs

Use these commands to manage policies and policy rules.

Policy APIs

- [clone_policy](#)
- [create_policy](#)
- [delete_policy](#)
- [list_installed_policies](#)
- [list_policy](#)
- [list_policy_rules](#)
- [policy_install](#)
- [policy_uninstall](#)

- [reinstall_policy](#)
- [reinstall_policy_rule](#)
- [rule_info_from_policy](#)
- [uninstall_policy_rule](#)
- [update_policy](#)

Policy Analyzer APIs

- [create_adhoc_policy_analyzer](#)
- [delete_adhoc_policy_analyzer](#)
- [disable_policy_analyzer](#)
- [enable_policy_analyzer](#)
- [get_policy_analyzer_status](#)
- [list_adhoc_policy_analyzer](#)
- [update_policy_analyzer_interval](#)

Rule APIs

- [add_receiver_to_rule_action](#)
- [change_rule_order](#)
- [copy_rule](#)
- [copy_rules](#)
- [create_rule](#)
- [create_rule_action](#)
- [delete_rule](#)
- [update_rule](#)

Process Control APIs

Use these commands to manage various process control functions.

- [close_default_events](#)
- [execute_appUserTranslation](#)
- [execute_assessment](#)
- [execute_incidentGenProcess](#)
- [execute_incidentGenProcess_byDetails](#)
- [execute_flatLogProcess](#)
- [execute_ldap_user_import](#)
- [export_log_files](#)
- [execute_populateGroupFromQuery](#)
- [get_flatLogProcessType](#)
- [get_ztap_logging_config](#)
- [kill_running_process](#)
- [list_health_node](#)
- [list_running_processes](#)
- [must_gather](#)
- [restart_job_queue_listener](#)
- [set_flatLogProcessType](#)
- [set_ztap_logging_config](#)
- [upload_custom_data](#)

Audit process APIs

- [audit_process_run_status](#)
- [delete_audit_process](#)
- [delete_audit_process_result](#)
- [execute_auditProcess](#)
- [list_audit_processes](#)
- [stop_audit_process](#)

Quarantine APIs

Use these APIs to manage quarantines for specified users. A user under quarantine cannot log in to the specified database.

- [create_quarantine_allowed_until](#)
- [create_quarantine_until](#)
- [delete_quarantine](#)
- [update_quarantine_allowed_until](#)
- [update_quarantine_until](#)

Query rewrite APIs

Use these commands to automate testing or create definitions for certain complex queries that cannot be done from the user interface.

Note: If you create query rewrite definitions by using APIs, you can still use the UI to retrieve those definitions for testing with the Query Rewrite Builder.

- [assign_gr_condition_to_action](#)
- [create_gr_action](#)
- [create_gr_add_where](#)
- [create_gr_add_where_by_id](#)
- [create_gr_condition](#)
- [create_gr_definition](#)
- [create_gr_replace_element](#)
- [create_gr_replace_element_byId](#)
- [list_gr_action](#)
- [list_gr_add_where](#)
- [list_gr_add_where_by_id](#)
- [list_gr_condition](#)
- [list_gr_condition_to_action](#)
- [list_gr_definitions](#)
- [list_gr_replace_element](#)
- [list_gr_replace_element_byId](#)
- [remove_all_gr_replace_elements](#)
- [remove_all_gr_replace_elements_byId](#)
- [remove_gr_action](#)
- [remove_gr_add_where_by_id](#)
- [remove_gr_condition](#)
- [remove_gr_definition](#)
- [remove_gr_replace_element_byId](#)
- [unassign_gr_condition_from_action](#)
- [update_gr_action](#)
- [update_gr_add_where_by_id](#)
- [update_gr_condition](#)
- [update_gr_definition](#)
- [update_gr_replace_element_byId](#)

Related concepts

- [Query rewrite](#)

Related reference

- [Windows S-TAP Query rewrite parameters](#)
 - [Linux-Unix S-TAP Query rewrite parameters](#)
-

Reports and report generation APIs

Use report generation APIs to manage reports and distributed reports, and to take the output from one Guardium® report or entity and feed it as the input for another Guardium entity.

Report APIs

Use these APIs to see the reports on a Guardium system, and to set or view parameters used in reports:

- [list_all_reports](#)
- [list_parameter_names_by_report_name](#)
- [show_maximum_query_duration](#)
- [store_maximum_query_duration](#)

Distributed report APIs

Use these APIs to manage distributed reports:

- [cancel_distributed_report_target](#)
- [delete_distributed_report_result_for_period](#)
- [get_distributed_report_target_info](#)
- [rerun_distributed_report](#)
- [set_distributed_report_target](#)

Ad hoc audit APIs

You can invoke the ad hoc audit APIs automatically from any report.

- [create_ad_hoc_audit_and_run_once](#)
- [create_ad_hoc_audit_and_run_with_name](#)
- [create_ad_hoc_audit_for_security_assessment](#)

Attribute and mapping APIs for reports

Use the following APIs to map API parameters to domain entities and attributes for reporting.

- [create_api_parameter_mapping](#)
- [create_computed_attribute](#)
- [create_constant_attribute](#)
- [delete_api_parameter_mapping](#)
- [delete_computed_attribute](#)
- [delete_constant_attribute](#)
- [disable_special_attributes](#)
- [enable_special_attributes](#)
- [list_param_mapping_for_function](#)
- [update_computed_attribute](#)
- [update_constant_attribute](#)

Related tasks

- [Working with API calls and reports](#)

Schedule and job dependencies APIs

Use these APIs to set schedules for and dependencies between jobs.

Job dependencies APIs

- [auto_execute_suggested_dependencies](#)
- [disable_auto_execute_suggested_dependencies](#)
- [list_existing_job_dependencies](#)
- [modify_job_dependency](#)
- [populate_from_dependencies](#)

Schedule APIs

- [add_all_to_schedule](#)
- [add_time_period](#)
- [delete_schedule](#)
- [list_schedules](#)
- [list_scheduler_jobs](#)
- [modify_schedule](#)
- [pause_or_resume_job](#)
- [remove_all_from_schedule](#)
- [schedule_job](#)

Related concepts

- [Scheduling](#)
- [Job dependencies](#)

Solr APIs

Run these commands on your central manager and managed units to manage their (internal Guardium) Solr database.

The Solr commands are:

- [get_solr_cluster_info](#)
- [getFieldsTitles](#)
- [get_solr_errors](#)
- [get_solr_status](#)
- [get_solr_status_extended](#)
- [restart_solr](#)
- [search](#)
- [stop_solr](#)
- [test_solr](#)
- [test_solr_connectivity](#)
- [test_solr_hardware_requirements](#)

Related information

- [Troubleshooting the investigation dashboard and enterprise search](#)

S-TAP and inspection engine APIs

Use these commands to manage your S-TAPs and their inspection engines.

- [add_approved_stap_client](#)
- [create_stap_inspection_engine](#)
- [delete_approved_stap_client](#)
- [delete_inactive_stap](#)
- [delete_invalid_stap](#)
- [delete_stap_inspection_engine](#)
- [display_stap_config](#)
- [list_approved_stap_client](#)
- [list_associated_stap_mu_groups](#)
- [list_engine_config](#)
- [list_inspection_engines](#)
- [list_staps](#)
- [list_stap_verification_results](#)
- [make_bundle_with_uploaded_kernel_module](#)
- [refresh_stap_info](#)
- [restart_stap](#)
- [revoke_ignore_stap](#)
- [set_ktap_debug](#)
- [set_stap_debug](#)
- [store_stap_approval](#)
- [update_engine_config](#)
- [update_stap_config](#)
- [verify_stap_inspection_engine_with_sequence](#)

S-TAP and Oracle Unified Auditing APIs

- [create_sql_configuration](#)
- [delete_sql_configuration](#)
- [store_sql_credentials](#)

S-TAP for IBM i APIs

Use these commands to create, list, delete, restart, and set i-S-TAP® functions.

The S-TAP for IBM i functions are:

- [get_istap_config](#)
- [get_istap_status](#)
- [start_istap_monitor](#)
- [stop_istap_monitor](#)
- [update_istap_config](#)

For more information, see [Db2 for IBM i S-TAP](#).

Threat detection analytics APIs

Use these GuardAPI commands to configure threat detection analytics.

The threat detection analytics commands are:

- [assign_analytic_case](#)
- [delete_analytic_user_feedback](#)
- [disable_advanced_threat_scanning](#)
- [disable_threat_detection_use_case](#)
- [enable_advanced_threat_scanning](#)
- [enable_threat_detection_use_case](#)
- [get_threat_detection_use_case_info](#)

Related concepts

- [Threat detection analytics](#)